512.74
L57q

UNIVERSITY OF ILLINOIS
LIBRARY

Class ~~512.814~~ 512.74 Book L57g Volume

My 08 15M

UNIVERSITY OF
ILLINOIS LIBRARY
AT URBANA-CHAMPAIGN
MATHEMATICS

QUELQUES DÉMONSTRATIONS

RELATIVES A LA

THÉORIE DES NOMBRES ENTIERS

COMPLEXES CUBIQUES

PROPRIÉTÉS

DE

QUELQUES GROUPES D'ORDRE FINI

Exemplaire N° 336

ANNALES DE L'UNIVERSITÉ DE LYON
NOUVELLE SÉRIE
I. *Sciences, Médecine.* — Fascicule 21.

QUELQUES DÉMONSTRATIONS
RELATIVES A LA
THÉORIE DES NOMBRES ENTIERS
COMPLEXES CUBIQUES

PROPRIÉTÉS
DE
QUELQUES GROUPES D'ORDRE FINI

PAR
RAYMOND LE VAVASSEUR
Professeur à la Faculté des Sciences de Lyon.

LYON
A. REY, IMPRIMEUR-ÉDITEUR
4, Rue Gentil

PARIS
LIBRAIRIE GAUTHIER-VILLARS
Quai des Grands-Augustins, 55

1908

UNIVERSITY OF ILLINOIS
LIBRARY

512.74
~~512.014~~
L579

QUELQUES DÉMONSTRATIONS

RELATIVES A LA

THÉORIE DES NOMBRES ENTIERS

COMPLEXES CUBIQUES.

114634

QUELQUES DÉMONSTRATIONS

RELATIVES A LA

THÉORIE DES NOMBRES ENTIERS

COMPLEXES CUBIQUES.

1. Les *nombres entiers complexes cubiques* sont les nombres $a + b\rho$, a et b étant des nombres entiers réels, positifs ou négatifs, ou nuls, et ρ étant l'une des racines de l'équation $\rho^2 + \rho + 1 = 0$.

Il y a six unités

$$1, \quad \rho, \quad \rho^2, \quad -1, \quad -\rho, \quad -\rho^2.$$

Les six nombres complexes cubiques obtenus en multipliant un nombre complexe entier cubique quelconque par les six unités sont dits *associés*. A l'exception de 0, qui est associé à lui-même, il y a toujours six associés différents.

La *norme* du nombre $a + b\rho$ est

$$a^2 - ab + b^2 = (a + b\rho)(a + b\rho^2).$$

La norme d'un produit de plusieurs facteurs est égale au produit des normes de ces facteurs.

2. Un nombre entier complexe cubique qui peut se décomposer en deux facteurs différents des unités sera dit *nombre complexe cubique composé*. Un nombre complexe cubique

premier sera un nombre qui n'admettra pas une telle décomposition.

Un nombre entier réel composé peut être regardé comme un nombre entier complexe cubique composé. Mais un nombre premier réel pourra être un nombre complexe cubique composé.

Ainsi $3 = (1 - \rho)(1 - \rho^2) = -\rho^2(1 - \rho)^2$ est composé.

Tout nombre premier de la forme $6h + 1$ est représentable par la forme $a^2 - ab + b^2$. Or

$$a^2 - ab + b^2 = (a + b\rho)(a + b\rho^2).$$

Ce sera donc un nombre complexe cubique composé. Ainsi

$$7 = (2 + 3\rho)(2 + 3\rho^2).$$

Au contraire, les nombres premiers réels de la forme $3n - 1$ *sont des nombres premiers complexes cubiques.*

En effet, si un tel nombre q était égal à $(a + b\rho)(\alpha + \beta\rho)$, on aurait aussi

$$q = (a + b\rho^2)(\alpha + \beta\rho^2).$$

Donc

$$q^2 = (a^2 - ab + b^2)(\alpha^2 - \alpha\beta + \beta^2).$$

Mais q^2 ne peut se décomposer en facteurs réels que d'une façon,

$$q^2 = qq;$$

donc

$$a^2 - ab + b^2 = \alpha^2 - \alpha\beta + \beta^2 = q.$$

Or les nombres premiers de la forme $3n - 1$ ne sont pas représentables par la forme $a^2 - ab + b^2$.

Donc q est complexe cubique premier.

3. Remarquons d'abord que, si deux nombres sont représentables par la forme $x^2 - xy + y^2$, il en sera de même de

leur produit. En effet, on a

$$\begin{aligned}&(a^2-ab+b^2)(\alpha^2-\alpha\beta+\beta^2)\\&\quad=(a\alpha-b\beta)^2-(a\alpha-b\beta)(a\beta+b\alpha-b\beta)+(a\beta+b\alpha-b\beta)^2\\&\quad=(a\beta-b\alpha)^2-(a\beta-b\alpha)(a\alpha+b\beta-b\alpha)+(a\alpha+b\beta-b\alpha)^2.\end{aligned}$$

Cela posé, établissons maintenant la proposition suivante :

Si un nombre premier p divise le nombre a^2-ab+b^2, il est lui-même de la forme $\alpha^2-\alpha\beta+\beta^2$.

En effet, supposons que p divise a^2-ab+b^2, où a et b sont premiers entre eux. Nous pouvons remplacer a et b par leurs restes minima (mod p). Nous désignerons par a', b' ces restes, inférieurs en valeur absolue à $\frac{p}{2}$.

On a

$$a'^2-a'b'+b'^2<3\left(\frac{p}{2}\right)^2<p^2.$$

On peut donc poser

$$a'^2-a'b'+b'^2=pp' \tag{1}$$

avec

$$p'<p.$$

Si p' était égal à 1, on aurait mis p sous la forme $a'^2-a'b'+b'^2$, et le théorème serait établi.

Supposons $p'>1$.

Soient $a'-\alpha p'$, $b'-\beta p'$ les restes minima de a' et de b' (mod p'). Ils ne sont pas nuls tous les deux; autrement, a' et b' ne seraient pas premiers entre eux; chacun d'eux est en valeur absolue égal ou inférieur à $\frac{p'}{2}$. Donc, on a

$$(a'-\alpha p')^2-(a'-\alpha p')(b'-\beta p')+(b'-\beta p')^2\leqq 3\frac{p'^2}{4}<p'^2$$

et, par suite, on peut poser

$$(a'-\alpha p')^2-(a'-\alpha p')(b'-\beta p')+(b'-\beta p')^2=p'p''$$

avec

$$p''<p'<p.$$

Donc

$$(a'^2 - a'b' + b'^2)[(a' - \alpha p')^2 - (a' - \alpha p')(b' - \beta p') + (b' - \beta p')^2] = pp'^2 p''$$

ou

$$A^2 - AB + B^2 = pp'^2 p''$$

avec

$$\begin{aligned} A &= a'(b' - \beta p') - b'(a' - \alpha p') = (b'\alpha - a'\beta)p' = a''p', \\ B &= a'(a' - \alpha p') + b'(b' - \beta p') - b'(a' - \alpha p') \\ &= a'^2 - a'b' + b'^2 - (a'\alpha + b'\beta - b'\alpha)p' \\ &= pp' - (a'\alpha + b'\beta - b'\alpha)p' \qquad = b''p'. \end{aligned}$$

Donc

$$(2) \qquad a''^2 - a''b'' + b''^2 = pp'',$$

égalité de la forme (1), avec

$$p'' < p'.$$

Si p'' est égal à 1, le théorème est démontré.

Si p'' n'est pas égal à 1, on opérera de même que tout à l'heure. On obtiendra une suite d'égalités de la forme

$$a_n^2 - a_n b_n + b_n^2 = pp_n$$

avec

$$p > p' > p'' > \ldots > p_n.$$

Pour n suffisamment grand, p_n sera égal à 1

4. Démontrons maintenant le théorème suivant :

Tout nombre entier cubique imaginaire $a + b\rho$ est un nombre premier ou un nombre composé suivant que la norme est elle-même un nombre premier ou composé.

1. Puisque, si l'on considère un nombre complexe cubique composé, la norme d'un tel nombre est le produit des normes des facteurs, on voit que ce sera aussi nécessairement un nombre composé. Il en résulte qu'*un nombre entier imagi-*

naire cubique dont la norme est un nombre premier réel est nécessairement premier.

Exemple. — $2 + 3\rho$ a pour norme 7. Donc $2 + 3\rho$ est premier.

2. Supposons que la norme $a^2 - ab + b^2$ soit un nombre composé. Soit p un nombre premier réel qui la divise. Alors deux cas sont à distinguer : si p est de la forme $3n - 1$, il ne peut diviser $a^2 - ab + b^2$ que s'il divise à la fois a et b (n° **3**).

Alors $a + b\rho$ est composé.

Si p est de la forme $6n + 1$, on peut poser

$$p = \alpha^2 - \alpha\beta + \beta^2.$$

Comme on a

$$(a\alpha - b\beta)(a\alpha + b\beta - a\beta) = a^2(\alpha^2 - \alpha\beta + \beta^2) - \beta^2(a^2 - ab + b^2),$$

puisque p divise le deuxième membre, il divise soit $a\alpha - b\beta$, soit $a\alpha + b\beta - a\beta$. Mais on a (n° **3**)

$$\begin{aligned}
&(a\alpha - b\beta)^2 - (a\alpha - b\beta)(a\beta + b\alpha - b\beta) + (a\beta + b\alpha - b\beta)^2 \\
&= (b\alpha - a\beta)^2 - (b\alpha - a\beta)(b\beta + a\alpha - a\beta) + (b\beta + a\alpha - a\beta)^2 \\
&= (ba - a\beta)^2 - (a\beta - b\alpha)(a\alpha + b\beta - b\alpha) + (a\alpha + b\beta - b\alpha)^2 \\
&= (a^2 - ab + b^2)(\alpha^2 - \alpha\beta + \beta^2).
\end{aligned}$$

Si p divise $a\alpha - b\beta$, il divise donc aussi $a\beta + b\alpha - b\beta$.

Si p divise $a\alpha + b\beta - a\beta$, il divise aussi $b\alpha - a\beta$.

Or

$$\frac{a + b\rho}{\alpha + \beta\rho} = \frac{a\alpha + b\beta - a\beta}{p} + \frac{b\alpha - a\beta}{p}\rho,$$

$$\frac{a + b\rho}{\alpha + \beta\rho^2} = \frac{a\alpha - b\beta}{p} + \frac{a\beta + b\alpha - b\beta}{p}\rho.$$

L'un ou l'autre des deux nombres $\frac{a + b\rho}{\alpha + \beta\rho}$, $\frac{a + b\rho}{\alpha + \beta\rho^2}$ sera donc entier. La norme du quotient, $\frac{a^2 - ab + b^2}{p}$, est, par hypothèse, différente de 1, puisque $a^2 - ab + b^2$ est un nombre composé. Donc $a + b\rho$ est un nombre composé.

Exemple : $5 + 11\rho$. La norme $25 - 55 + 121 = 91 = 7.13$. $5 + 11\rho$ est composé. En effet

$$5 + 11\rho = (2 + 3\rho)(4 + \rho).$$

5. Les nombres complexes cubiques premiers se partagent en quatre catégories :

1. Les six unités. La plupart du temps nous les exclurons des nombres premiers. [Remarquons que l'on a $1 = \rho\rho^2$, $-1 = \rho(1 + \rho)$, ...]

2. Le nombre $1 - \rho$ et ses associés, $1 + 2\rho$, $-2 - \rho$, $-1 + \rho$, $-1 - 2\rho$, $2 + \rho$.

3. Les nombres premiers réels positifs de la forme $3n - 1$ et leurs associés.

4. Les nombres imaginaires cubiques dont les normes sont des nombres premiers réels de la forme $6n + 1$.

Une norme de cette forme étant donnée, il lui correspond douze nombres imaginaires. Ainsi 7 donne $2 + 3\rho$, $-3 - \rho$, $1 - 2\rho$, $3 + 2\rho$, $-2 + \rho$, $-1 - 3\rho$, $-2 - 3\rho$, $3 + \rho$, $-1 + 2\rho$, $-3 - 2\rho$, $2 - \rho$, $1 + 3\rho$.

Elle n'en donne pas plus de 12, puisqu'elle ne peut être décomposée que d'une manière dans la forme $a^2 - ab + b^2$.

6. J'écarte les nombres divisibles par $1 - \rho$ (à un facteur-unité près).

Parmi les autres, avec Eisenstein (*J. de Crelle,* t. 27, p. 301), j'appelle *primaire* tout nombre $a + b\rho$ congru à 2 (mod 3).

Les cinq nombres associés à $a + b\rho$ sont $-b + (a - b)\rho$, $b - a - a\rho$, $-a - b\rho$, $b + (b - a)\rho$, $a - b + a\rho$.

Le Tableau suivant, où figurent les restes (mod 3) des six nombres associés va montrer que sur ces six nombres associés

il n'y a qu'un nombre primaire :

a.	b.	$-b$.	$a-b$.	$b-a$.	$-a$.	Nombre primaire.
0	0	0	0	0	0	(Exclu)
0	1	2	2	1	0	$a-b+a\rho$
0	2	1	1	2	0	$b-a-a\rho$
1	0	0	1	2	2	$-a-b\rho$
1	1	2	0	0	2	$-b+(a-b)\rho$
1	2	1	2	1	2	(Exclu)
2	0	0	2	1	1	$a+b\rho$
2	1	2	1	2	1	(Exclu)
2	2	1	0	0	1	$b+(b-a)\rho$

Les nombres exclus sont divisibles par $(1-\rho)$, car

$$3\alpha+1+(3\beta+2)\rho=3(\alpha+\beta\rho)+1+2\rho$$

est divisible par $1+2\rho$,

$$3\alpha+2+(3\beta+1)\rho=3(\alpha+\beta\rho)+2+\rho$$

est divisible par $2+\rho$; or $1+2\rho$, $2+\rho$ sont des associés de $1-\rho$ (n° 5).

7. Si, parmi les facteurs d'un nombre complexe cubique il en est qui soient eux-mêmes composés, on peut les décomposer en facteurs, et l'on arrivera nécessairement, à la fin, à n'avoir que des facteurs premiers. S'il en est qui ne soient pas primaires, on leur substituera le facteur primaire associé à condition de mettre en facteur un nombre $(-1)^\lambda\rho^\mu$ convenablement choisi. Le nombre complexe composé M pourra donc être mis sous la forme

$$M=(-1)^\lambda\rho^\mu(1-\rho)^\nu A^\alpha B^\beta C^\gamma\ldots,$$

où A, B, C sont des nombres complexes cubiques premiers primaires inégaux.

Nous regarderons $1-\rho$ comme primaire.

Théorème. — *Le produit* $M = A^\alpha B^\beta C^\gamma \ldots L^\lambda$, *où* A, B, C, ..., L *désignent des nombres complexes cubiques premiers primaires différents, ne peut être divisible par aucun autre nombre complexe cubique premier primaire que* A, B, C, ..., L.

Soit, en effet, P un nombre premier complexe cubique primaire non contenu parmi les nombres A, B, C, ..., L.

Soient p, a, b, c, ..., l les normes des nombres P, A, B, C, ..., L.

La norme de M est $a^\alpha b^\beta c^\gamma \ldots l^\lambda$.

Si M est divisible par P, la norme de M est divisible par p.

La norme d'un nombre complexe cubique est soit un nombre premier réel de la forme $6n + 1$ (7, 13, 19, ...), soit le carré d'un nombre premier réel de la forme $3n - 1$ (4, 25, 121, ...), ou enfin 3.

p sera donc nécessairement égal à l'une des normes a, b, c, ..., l.

Supposons $p = a$. Si nous observons que deux nombres complexes imaginaires conjugués $m + n\rho$, $m + n\rho^2$ sont simultanément primaires, comme P et A sont, par hypothèse, des nombres premiers complexes cubiques primaires non identiques, P et A sont nécessairement imaginaires conjugués (nos **5** et **6**). Donc $p = a$ est un nombre premier réel de la forme $6n + 1$ [on n'a pas $p = 3$, car $1 - \rho^2 = 2 + \rho$ est associé de $(1 - \rho)$], $p = a$ n'est pas le carré d'un nombre premier.

Soit donc

$$A = r + s\rho, \qquad P = r + s\rho^2.$$

On a

$$A = r - s - s\rho^2 = 2r - s - (r + s\rho^2)$$

ou

$$A \equiv 2r - s \pmod{P}.$$

Donc

$$M \equiv (2r - s)^\alpha B^\beta C^\gamma \ldots L^\lambda \pmod{P}.$$

Nous supposons M divisible par P.

Donc $(2r-s)^{\alpha}B^{\beta}C^{\gamma}\ldots L^{\lambda}$ sera divisible par P.

Sa norme $(2r-s)^{2\alpha}b^{\beta}c^{\gamma}\ldots l^{\lambda}$ sera donc divisible par $p=r^2-rs+s^2$.

Comme ni r ni s ne sont divisibles par p, l'identité

$$4p=(2r-s)^2+3s^2$$

nous montre que $2r-s$ n'est pas divisible par p.

p devrait donc être identique à l'un des autres nombres b, c, ..., l; soit, par exemple, $p=b$.

On en conclurait

$$B=r+s\rho \qquad \text{ou} \qquad B=r+s\rho^2,$$

c'est-à-dire

$$B=A \qquad \text{ou} \qquad B=P.$$

L'une et l'autre conclusion sont inadmissibles.

Donc le théorème est démontré.

De ce théorème on déduirait, comme dans le cas des nombres naturels, que la décomposition en facteurs premiers complexes cubiques primaires n'est possible que d'une façon.

8. *Relativement à un module complexe cubique donné, $m=a+b\rho$, dont la norme est $a^2-ab+b^2=p$, et pour lequel a et b sont des nombres premiers entre eux, tout nombre entier complexe cubique sera congru à un nombre, et à un seul, de la suite* 0, 1, 2, ..., $p-1$.

En effet :

1. a et b étant premiers entre eux, il existe des nombres entiers α et β tels que l'on ait

$$a\alpha+b\beta=1.$$

Remarquons alors que l'on a

$$\rho=\alpha b-(\alpha+\beta)a+m(\alpha+\beta+\alpha\rho).$$

Soit maintenant $A+B\rho$ un nombre complexe cubique quelconque.

On aura

$$A + B\rho = A + [\alpha b - (\alpha + \beta)a]B + m[(\alpha + \beta)B + \alpha B\rho].$$

Soit h le reste minimum positif de $A + [\alpha b - (\alpha + \beta)a]B$ suivant le module

$$p = (a + b\rho)(a + b\rho^2) = (a + b\rho^2)m.$$

On a

$$A + [\alpha b - (\alpha + \beta)a]B = h + kp = h + km(a + b\rho^2).$$

Donc

$$A + B\rho = h + m[k(a + b\rho^2) + (\alpha + \beta + \alpha\rho)B]$$

ou

$$A + B\rho \equiv h \qquad (\bmod m).$$

2. *Toutes les fois que les deux nombres réels h et h' sont congrus suivant le module $m = a + b\rho$ à un même nombre complexe cubique, ils sont aussi congrus suivant la norme p de m.*

En effet, posons

$$h - h' = m(c + d\rho^2) \qquad (m = a + b\rho),$$

d'où

$$(h - h')(a + b\rho^2) = p(c + d\rho^2).$$

On a, par suite,

$$(h - h')a = pc, \qquad (h - h')b = pd.$$

Comme $a\alpha + b\beta = 1$, il vient

$$h - h' = p(c\alpha + d\beta).$$

Donc

$$h \equiv h' \qquad (\bmod p).$$

C'est pourquoi, si h et h' ne sont pas égaux, ils ne peuvent être simultanément contenus dans la suite $0, 1, 2, \ldots, p - 1$.

9. *Si l'on prend pour module complexe cubique,* $m = a + b\rho$, *un nombre dont la norme est* $p = a^2 - ab + b^2$ *et pour lequel* a *et* b *ne sont pas premiers entre eux, mais admettent le plus grand commun diviseur* λ (on pourra supposer que λ est un nombre naturel), *un nombre complexe cubique quelconque sera congru au reste* $x + yi$ *tel que* x *soit l'un des nombres* $0, 1, 2, 3, \ldots, \frac{p}{\lambda} - 1$, *et* y *l'un des nombres* $0, 1, 2, \ldots, \lambda - 1$, *et ce reste sera le seul entre les* p *restes de la même forme auquel puisse être congru le nombre complexe cubique considéré.*

1. Soient α et β des nombres entiers relatifs tels que l'on ait

$$\alpha a + \beta b = \lambda.$$

Alors on aura

$$\lambda\rho = \alpha b - (\alpha + \beta)a + m(\alpha + \beta + \alpha\rho) \qquad (\text{n}^{\circ}\ \mathbf{8}).$$

Soit $A + B\rho$ le nombre complexe cubique proposé.

Appelons y le reste minimum positif de B suivant le module λ, et x le reste minimum positif de

$$A + [\alpha b - (\alpha + \beta)a]\frac{B - y}{\lambda} \qquad \left[\operatorname{mod}\left(\frac{p}{\lambda}\right)\right].$$

On pourra poser

$$A + [\alpha b - (\alpha + \beta)a]\frac{B - y}{\lambda} = x + \frac{p}{\lambda}k,$$

$$A - x = \frac{p}{\lambda}k + [(\alpha + \beta)a - \alpha b]\frac{B - y}{\lambda},$$

ou

$$A - x + (B - y)\rho = \frac{p}{\lambda}k + (B - y)\rho + [(\alpha + \beta)a - \alpha b]\frac{B - y}{\lambda},$$

ou

$$A + B\rho - (x + y\rho) = \frac{p}{\lambda}k + \frac{B - y}{\lambda}[\lambda\rho + (\alpha + \beta)a - \alpha b].$$

ou

$$A + B\rho - (x + y\rho) = \frac{(a + b\rho^2)mk}{\lambda} + \frac{B - y}{\lambda}m(\alpha + \beta + \alpha\rho).$$

Donc

$$A + B\rho \equiv x + y\rho \pmod{m}.$$

2. Supposons que les deux nombres $x + y\rho$, $x' + y'\rho$ soient congrus suivant le module m à un même nombre complexe cubique, et, par conséquent, congrus entre eux $(\bmod m)$. Ils seront, par suite, congrus entre eux $(\bmod \lambda)$. Donc on aura

$$y \equiv y' \pmod{\lambda}.$$

De là suit que, si y et y' sont supposés tous les deux contenus dans la suite $0, 1, 2, \ldots, \lambda - 1$, il faudra que l'on ait

$$y = y'.$$

Mais alors on aura

$$x \equiv x' \pmod{m};$$

$x - x'$ sera divisible par m. Donc le nombre $\frac{x - x'}{\lambda}$, qui est entier, sera divisible par $\frac{a}{\lambda} + \frac{b}{\lambda}\rho$.

On aura

$$\frac{x - x'}{\lambda} \equiv 0 \left[\bmod \left(\frac{a}{\lambda} + \frac{b}{\lambda}\rho\right)\right].$$

Mais, comme $\frac{a}{\lambda}$, $\frac{b}{\lambda}$ sont des nombres premiers entre eux, il suit de la deuxième partie du théorème précédent (n° **8**) que $\frac{x - x'}{\lambda}$ est divisible par la norme de $\frac{a}{\lambda} + \frac{b}{\lambda}\rho$, c'est-à-dire par $\frac{p}{\lambda^2}$, de sorte que $x - x'$ est divisible par $\frac{p}{\lambda}$. Donc, si x et x' sont tous les deux contenus dans la suite $0, 1, 2, \ldots, \frac{p}{\lambda} - 1$, on aura nécessairement

$$x = x'.$$

Les restes $x + \rho y$, $x' + \rho y'$ sont donc identiques.

A ce cas, d'ailleurs, on peut rapporter soit le cas $b = 0$,

$\lambda = \pm a$, soit le cas $a = 0$, $\lambda = \pm b$. On a alors

$$\frac{p}{\lambda} = \lambda.$$

10. Les démonstrations qui précèdent sont, pour la plupart, calquées sur les démonstrations analogues faites par Gauss dans sa théorie des nombres entiers complexes de la forme $a + bi$ (2e Mémoire sur les restes biquadratiques, *Œuvres*, t. II).

Ces préliminaires posés, le lecteur est en mesure de lire le Mémoire d'Eisenstein sur la loi de réciprocité pour le cas des nombres complexes entiers cubiques (*J. de Crelle*, t. 27, p. 289), et le Mémoire de Stieltjes sur le même sujet (*Annales de la Faculté des Sciences de Toulouse*, 1897).

J'adopte, dans ce qui va suivre, les notations de ces deux auteurs. Je vais démontrer quelques propositions énoncées dans le Mémoire de Stieltjes, sans démonstration (n° **33**). Les modules que je considère sont toujours, par hypothèse, des nombres premiers.

11. Soit Q un nombre premier de la forme $6n - 1$.

On a

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{a + b\rho}{Q}\right] \qquad \text{(Eisenstein, } \textit{loc. cit.}\text{)}.$$

Si l'on a $a \equiv 0 \pmod{Q}$, comme $\left[\frac{b}{Q}\right] = 1$ (Eisenstein, *loc. cit.*),

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{\rho}{Q}\right] = \rho^{\frac{1}{3}(Q^2-1)} = \rho^{4n(3n-1)} = \rho^{2n}.$$

On peut donc dire :

$6n - 1$ étant premier, ainsi que $\alpha(6n - 1) + b\rho$, on a

$$\left[\frac{6n - 1}{\alpha(6n - 1) + b\rho}\right] = \rho^{2n}.$$

12. Soit $P = 6n + 1$ un nombre premier :

$$P = (M + N\rho)(M + N\rho^2),$$

$$\left[\frac{P}{a + b\rho}\right] = \left[\frac{a + b\rho}{P}\right].$$

Si l'on a $a \equiv 0 \pmod{P}$, comme $\left[\frac{b}{P}\right] = 1$, il vient

$$\left[\frac{P}{a + b\rho}\right] = \left[\frac{\rho}{P}\right] = \left[\frac{\rho}{M + N\rho}\right]\left[\frac{\rho}{M + N\rho^2}\right] = \rho^{\frac{2}{3}(P-1)} = \rho^{4n} = \rho^n.$$

On peut dire :

$6n + 1$ étant premier réel et $\alpha(6n + 1) + b\rho$ étant un module complexe cubique premier, on a

$$\left[\frac{6n + 1}{\alpha(6n + 1) + b\rho}\right] = \rho^n.$$

13. Si $b \equiv 0 \pmod{Q}$, Q étant un nombre premier de la forme $6n - 1$, on a

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{Q}{a + \beta Q\rho}\right] = \left[\frac{a + \beta Q\rho}{Q}\right] = \left[\frac{a}{Q}\right] = 1.$$

De même, si $b \equiv 0 \pmod{P}$, P étant un nombre premier de la forme $6n + 1$, on a

$$\left[\frac{P}{a + b\rho}\right] = \left[\frac{P}{a + \beta P\rho}\right] = \left[\frac{a + \beta P\rho}{P}\right] = \left[\frac{a}{P}\right] = 1.$$

14. Si $b \equiv 2a \pmod{Q}$,

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{a(1 + 2\rho)}{Q}\right] = \left[\frac{a}{Q}\right]\left[\frac{1 + 2\rho}{Q}\right] = \left[\frac{1 + 2\rho}{Q}\right].$$

Or

$$\frac{1}{3}(Q^2 - 1) = \frac{1}{3}(Q + 1)(Q - 1) = 2n(Q - 1),$$

$$(1 + 2\rho)^{2n} = (-3)^n.$$

Mais

$$(-3)^{n(Q-1)} \equiv 1 \qquad (\bmod Q) \qquad (\text{théorème de Fermat});$$

donc, *si* $b \equiv 2a \pmod{Q}$, Q *appartient à la classe* A.

15. Soit $b \equiv 2a \pmod{P}$, P étant un nombre premier de la forme $6n+1$:

$$P = 6n+1 = (\mu+\nu\rho)(\mu+\nu\rho^2),$$

$$\left[\frac{P}{a+b\rho}\right] = \left[\frac{a(1+2\rho)}{P}\right] = \left[\frac{a}{P}\right]\left[\frac{1+2\rho}{P}\right].$$

Mais

$$\left[\frac{a}{P}\right] = \left[\frac{a}{\mu+\nu\rho}\right]\left[\frac{a}{\mu+\nu\rho^2}\right] = 1 \qquad (\textit{voir } \text{EISENSTEIN}, \textit{loc. cit.});$$

donc

$$\left[\frac{P}{a+b\rho}\right] = \left[\frac{1+2\rho}{P}\right] = \left[\frac{1+2\rho}{\mu+\nu\rho}\right]\left[\frac{1+2\rho}{\mu+\nu\rho^2}\right] = \left[\frac{(1+2\rho)(1+2\rho^2)^2}{\mu+\nu\rho}\right].$$

On a

$$(1+2\rho^2)^2 = 1+4\rho^2+4\rho^4 = 1+4\rho^2+4\rho = -3,$$

$$\left[\frac{P}{a+b\rho}\right] = \left[\frac{-3-6\rho}{\mu+\nu\rho}\right] = (-3-6\rho)^{\frac{1}{3}(P-1)} = (-3-6\rho)^{2n}.$$

Or

$$(-3-6\rho)^2 = 9+36\rho+36\rho^2 = -27,$$

$$(-27)^n = (-3)^{3n}.$$

D'autre part, on sait que -3 est reste quadratique de $P = 6n+1$; on a donc

$$-3 \equiv \alpha^2, \qquad (-3)^{3n} \equiv \alpha^{6n} = \alpha^{P-1} \equiv 1 \qquad (\bmod P).$$

Bref, P *appartient à la classe* A $[\bmod(a+b\rho)]$.

Des deux propriétés des n^{os} **14** et **15**, et de ce fait si $p = a^2 - ab + b^2$ on a

$$4p = (2a-b)^2 + 3b^2,$$

de sorte que 3 ne divise pas $a - b$, Stieltjes a conclu (*loc. cit.*) que *tous les facteurs premiers de* $2a - b$ *et* $(2a - b)$ *lui-même sont restes cubiques de* p.

16. Soit Q un nombre premier de la forme $6n - 1$.

J'envisage toujours un module complexe cubique premier $a + b\rho$.

Si, pour $a \equiv 0 \pmod{Q}$, Q *appartient à la classe* A, Q *appartient aussi à la classe* A *lorsque* $b \equiv a$, *ou lorsque* $b \equiv -a \pmod{Q}$.

En effet, si, pour $a \equiv 0 \pmod{Q}$, Q appartient à A, alors (n° **11**) $n = 3\nu$, et l'on a

$$Q = 18\nu - 1.$$

Si $b \equiv a \pmod{Q}$,

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{a(1+\rho)}{Q}\right].$$

Mais

$$\left[\frac{a}{Q}\right] = 1;$$

donc

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{1+\rho}{Q}\right] = (1+\rho)^{\frac{1}{3}(Q^2-1)}.$$

Or

$$\frac{1}{3}(Q^2 - 1) = \frac{1}{3}(Q+1)(Q-1) = 6\nu(Q-1)$$

et

$$(1+\rho)^2 = 1 + 2\rho + \rho^2 = \rho, \qquad (1+\rho)^{6\nu} = \rho^{3\nu} = 1;$$

donc Q appartient à la classe A $[\mathrm{mod}(a + b\rho)]$.

Si $b \equiv -a \pmod{Q}$,

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{a(1-\rho)}{Q}\right] = \left[\frac{1-\rho}{Q}\right] = (1-\rho)^{\frac{1}{3}(Q^2-1)},$$

$$(1-\rho)^2 = 1 - 2\rho + \rho^2 = -3\rho, \qquad (-3\rho)^{3\nu} = (-27)^{\nu}.$$

Mais

$$(-27)^{\nu(Q-1)} \equiv 1 \pmod{Q} \qquad \text{(théorème de Fermat)};$$

donc Q appartient à la classe A.

17. *Si, pour* $a \equiv 0 \pmod{Q}$, Q *appartient à la classe* B, Q *appartient à la classe* C *lorsque* $b \equiv a$ *ou lorsque* $b \equiv -a \pmod{Q}$.

En effet, si pour $a \equiv 0 \pmod{Q}$, Q appartient à B, on a (n° **11**)

$$2n \equiv 1 \pmod{3}, \qquad n = 2 + 3\nu, \qquad Q = 12 + 18\nu - 1 = 18\nu + 11,$$

$$\frac{1}{3}(Q+1) = 6\nu + 4 = 2(3\nu + 2), \qquad Q - 1 = 2(9\nu + 5).$$

Si $b \equiv a \pmod{Q}$,

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{a(1+\rho)}{Q}\right] = \left[\frac{1+\rho}{Q}\right] = (1+\rho)^{\frac{1}{3}(Q^2-1)},$$

$$(1+\rho)^{\frac{1}{3}(Q^2-1)} = \rho^{2(3\nu+2)(9\nu+5)} = \rho^{20} = \rho^2;$$

donc Q appartient à la classe C.

Si $b \equiv -a \pmod{Q}$,

$$\left[\frac{Q}{a + b\rho}\right] = \left[\frac{a(1-\rho)}{Q}\right] = \left[\frac{1-\rho}{Q}\right] = (1-\rho)^{\frac{1}{3}(Q^2-1)},$$

$$(1-\rho)^{\frac{1}{3}(Q^2-1)} = (1-\rho)^{2(3\nu+2)(Q-1)} = (-3)^{(3\nu+2)(Q-1)}\rho^2.$$

D'ailleurs on a

$$(-3)^{(3\nu+2)(Q-1)} \equiv 1 \pmod{Q};$$

donc Q appartient à la classe C.

18. *Si, pour* $a \equiv 0 \pmod{Q}$, Q *appartient à la classe* C, Q *appartient à la classe* B *lorsque* $b \equiv a$ *ou lorsque* $b \equiv -a \pmod{Q}$.

En effet, si, pour $a \equiv 0 \pmod{Q}$, Q appartient à C, on a (n° **11**)

$$n \equiv 1 \pmod{3}, \qquad n = 1 + 3\nu, \qquad Q = 18\nu + 5,$$

$$\frac{1}{3}(Q+1) = 2(3\nu+1), \qquad Q - 1 = 2(9\nu+2).$$

Si $b \equiv a \pmod{Q}$,

$$\left[\frac{Q}{a+b\rho}\right] = (1+\rho)^{\frac{1}{3}(Q^2-1)},$$

$$(1+\rho)^{4(3\nu+1)(9\nu+2)} = \rho^{2(3\nu+1)(9\nu+2)} = \rho^4 = \rho;$$

donc Q appartient à la classe B.

Si $b \equiv -a \pmod{Q}$,

$$\left[\frac{Q}{a+b\rho}\right] = (1-\rho)^{\frac{1}{3}(Q^2-1)},$$

$$(1-\rho)^{\frac{1}{3}(Q^2-1)} = (-3\rho)^{(3\nu+1)(Q-1)}.$$

Mais

$$(-3)^{(3\nu+1)(Q-1)} \equiv 1 \pmod{Q};$$

donc

$$(1-\rho)^{\frac{1}{3}(Q^2-1)} \equiv \rho \pmod{Q},$$

Q appartient à B.

19. Il nous reste à démontrer les mêmes théorèmes dans le cas d'un nombre premier, P, de la forme $6n+1$.

Alors

$$\left[\frac{P}{\alpha P + b\rho}\right] = \rho^n \qquad \text{si} \qquad P = 6n+1 \qquad (\text{n° } \mathbf{9}).$$

Si, pour $a \equiv 0 \pmod{P}$, P appartient à A,

$$n = 3\nu \qquad \text{et} \qquad P = 18\nu + 1 = (\alpha + \beta\rho)(\alpha + \beta\rho^2).$$

Si $b \equiv a \pmod{P}$,

$$\left[\frac{P}{a+b\rho}\right] = \left[\frac{a(1+\rho)}{P}\right]$$

$$= \left[\frac{1+\rho}{P}\right] = \left[\frac{1+\rho}{\alpha+\beta\rho}\right]\left[\frac{1+\rho}{\alpha+\beta\rho^2}\right] = \left[\frac{(1+\rho)(1+\rho^2)^2}{\alpha+\beta\rho}\right],$$

$$(1+\rho^2)^2 = 1+2\rho^2+\rho = \rho^2, \qquad (1+\rho)\rho^2 = 1+\rho^2,$$

$$\left[\frac{P}{a+b\rho}\right] = (1+\rho^2)^{\frac{1}{3}(P-1)} = (1+\rho^2)^{6\nu} = \rho^{6\nu} = 1;$$

donc P appartient à A.

Si $b \equiv -a \pmod{P}$,

$$\left[\frac{P}{a+b\rho}\right] = \left[\frac{a(1-\rho)}{P}\right] = \left[\frac{1-\rho}{P}\right] = \left[\frac{(1-\rho)(1-\rho^2)^2}{\alpha+\beta\rho}\right]$$

$$= \left[\frac{3(1-\rho^2)}{\alpha+\beta\rho}\right] = \left(3(1-\rho^2)\right)^{\frac{1}{3}(P-1)} = 3^{6\nu}(1-\rho^2)^{6\nu}$$

$$= 3^{6\nu}(-3\rho^2)^{3\nu} = (-3)^{3\nu}3^{6\nu} = (-3)^{9\nu}.$$

Or, -3 est reste quadratique de P.

Soit

$$-3 \equiv m^2 \pmod{P}, \qquad (-3)^{9\nu} \equiv m^{18\nu} = m^{P-1} \equiv 1 \pmod{P};$$

donc P appartient à la classe A.

20. Si, pour $a \equiv 0 \pmod{P}$, P appartient à B,

$$n = 3\nu + 1,$$

$$P = (\alpha+\beta\rho)(\alpha+\beta\rho^2) = 18\nu + 7.$$

Si $b \equiv a \pmod{P}$,

$$\left[\frac{P}{a+b\rho}\right] = (1+\rho^2)^{\frac{1}{3}(P-1)} = (1+\rho^2)^{2(3\nu+1)} = \rho^2;$$

donc P appartient à la classe C.

Si $b \equiv -a \pmod{P}$,

$$\left[\frac{P}{a+b\rho}\right] = \left(3(1-\rho^2)\right)^{\frac{1}{3}(P-1)}$$
$$= \left(3(1-\rho^2)\right)^{2(3\nu+1)} = 3^{2(3\nu+1)}(-3)^{3\nu+1}\rho^3 = (-3)^{3(3\nu+1)}\rho^2,$$
$$P = 18\nu + 7 = 6\sigma + 1;$$

-3 est reste quadratique de P.

Donc, si $-3 \equiv m^2 \pmod{P}$,

$$(-3)^{3(3\nu+1)} = m^{P-1} \equiv 1 \pmod{P};$$

donc P appartient à la classe C.

21. Si, pour $a \equiv 0 \pmod{P}$, P appartient à C,

$$n = 3\nu + 2,$$
$$P = (\alpha + \beta\rho)(\alpha + \beta\rho^2) = 18\nu + 13.$$

Si $b \equiv a \pmod{P}$,

$$\left[\frac{P}{a+b\rho}\right] = (1+\rho^2)^{\frac{1}{3}(P-1)} = (1+\rho^2)^{2(3\nu+2)} = \rho^4 = \rho;$$

donc P appartient à la classe B.

Si $b \equiv -a \pmod{P}$,

$$\left[\frac{P}{a+b\rho}\right] = \left(3(1-\rho^2)\right)^{2(3\nu+2)} = (-3)^{3(3\nu+2)}\rho.$$

Mais

$$P = 18\nu + 13 = 6\sigma + 1,$$

-3 est reste quadratique de P.

Si $-3 \equiv m^2 \pmod{P}$,

$$(-3)^{3(3\nu+2)} = m^{P-1} \equiv 1 \pmod{P};$$

donc P appartient à la classe B.

PROPRIÉTÉS

DE

QUELQUES GROUPES D'ORDRE FINI.

PROPRIÉTÉS

DE

QUELQUES GROUPES D'ORDRE FINI.

1. *Groupes cycliques d'ordre p, p étant premier.* — Soit le groupe G_p, d'ordre p, p étant premier.

Il a pour équation de définition

$$a^p = 1.$$

Il y a une seule opération génératrice, l'opération a, d'ordre p.

Le groupe régulier de substitutions correspondant sera engendré par la substitution

$$(1, 2, \ldots, p).$$

La Table de multiplication sera [1]

$$\left|\begin{array}{ccccc} 1 & a & a^2 & \ldots & a^{p-1} \\ a^{p-1} & 1 & a & \ldots & a^{p-2} \\ a^{p-2} & a^{p-1} & 1 & \ldots & a^{p-3} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a & a^2 & a^3 & \ldots & 1 \end{array}\right|.$$

[1] *Voir* le Mémoire publié en 1904, *Annales de l'Université de Lyon* (fasc. 15).

Soient a^λ, a^μ deux opérations quelconques du groupe. On a

$$a^\lambda a^\mu = a^{\lambda+\mu}.$$

L'exposant de a est un nombre entier pris suivant le module p.

Telle est la loi de multiplication.

J'en déduis

$$a^\lambda = \begin{pmatrix} a^x \\ a^{x+\lambda} \end{pmatrix} \qquad (x = 1, 2, \ldots, p),$$

symbole qui représentera clairement chaque opération.

Il y a, dans le gronpe $\{a\}$, $p-1$ opérations d'ordre p.

Il y a deux sous-groupes, le groupe lui-même et le groupe formé de l'opération identique. Le groupe G_p est un groupe simple.

Chaque opération de G_p est conjuguée d'elle-même.

Le groupe des isomorphismes cogrédients se réduit à l'opération identique, comme pour tout groupe abélien.

Cherchons le groupe total des isomorphismes.

On pourra prendre comme opération génératrice l'une quelconque des $(p-1)$ opérations d'ordre p.

De là, $p-1$ isomorphismes :

$$b_\lambda = \begin{pmatrix} a \\ a^\lambda \end{pmatrix} \qquad (\lambda = 1, 2, \ldots, p-1).$$

Ainsi le groupe total des isomorphismes est d'ordre $p-1$.

On a

$$b_\lambda = \begin{pmatrix} a^x \\ a^{\lambda x} \end{pmatrix},$$

$$b_\lambda^\alpha = \begin{pmatrix} a^x \\ a^{x\lambda^\alpha} \end{pmatrix}.$$

Pour qu'on ait $b_\lambda^\alpha = 1$, il faut

$$\lambda^\alpha \equiv 1 \qquad (\bmod p).$$

Or, nous pouvons supposer que λ appartient à l'exposant $p-1 \pmod{p}$. Alors b_λ est d'ordre $p-1$.

Le groupe des isomorphismes est donc un groupe cyclique d'ordre $p-1$.

2. *Groupes cycliques d'ordre quelconque n.* — Soit G_n le groupe cyclique d'ordre n, n étant un nombre entier quelconque. Il a, pour unique équation de définition,

$$a^n = 1.$$

Il n'a qu'une seule opération génératrice, l'opération a, d'ordre n. Mais on peut trouver d'autres modes de génération, comme nous le verrons tout à l'heure.

Le groupe régulier correspondant sera engendré par la substitution $(1, 2, \ldots, n)$.

La Table de multiplication est

$$\begin{vmatrix} 1 & a & a^2 & \ldots & a^{n-1} \\ a^{n-1} & 1 & a & \ldots & a^{n-2} \\ a^{n-2} & a^{n-1} & 1 & \ldots & a^{n-3} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a & a^2 & a^3 & \ldots & 1 \end{vmatrix}.$$

Ce n'est pas, d'ailleurs, la seule manière de l'écrire, comme nous le verrons plus tard.

On a

$$a^\lambda a^\mu = a^{\lambda+\mu}$$

ou

$$a^\lambda = \begin{pmatrix} a^x \\ a^{x+\lambda} \end{pmatrix} \qquad (x = 1, 2, \ldots, n).$$

Les exposants sont pris suivant le module n.

3. Il y a, dans le groupe $\{a\}$, $\varphi(d)$ opérations d'ordre d; d représente l'un quelconque des diviseurs de n; $\varphi(d)$ est le nombre des entiers inférieurs à d et premiers avec d. [On suppose $\varphi(1) = 1$.]

Comme on a

$$n = \Sigma \varphi(d),$$

le signe Σ s'étendant à tous les diviseurs de n, on voit qu'il n'y a qu'*un* sous-groupe d'ordre d; ce sous-groupe sera un sous-groupe cyclique.

On a ainsi *tous* les sous-groupes du groupe cyclique considéré.

Ainsi, un groupe cyclique n'admet que des sous-groupes cycliques; il y a autant de sous groupes que n admet de diviseurs.

Soit α un nombre premier avec n : les seuls isomorphismes possibles sont de la forme

$$A_\alpha = \begin{pmatrix} a^x \\ a^{\alpha x} \end{pmatrix} \qquad (x = 1, 2, \ldots, n);$$

β étant un nombre premier avec n, on a

$$A_\alpha A_\beta = A_\beta A_\alpha = A_{\alpha\beta}.$$

Or les nombres entiers premiers avec n et pris suivant le module n forment un groupe Γ, d'ordre $\varphi(n)$.

Donc, le groupe des isomorphismes A_α sera d'ordre $\varphi(n)$ et simplement isomorphe avec le groupe Γ. Ce sera donc un groupe abélien.

4. Si n est de la forme p^m, p étant premier impair, il existera un nombre entier λ, appartenant à l'exposant

$$\varphi(p^m) = p^{m-1}(p-1) \qquad (\bmod p^m).$$

Alors le groupe des isomorphismes sera un groupe cyclique.

5. Soient

$$n = m_1 m_2 \ldots m_r,$$

les facteurs $m_1, m_2, \ldots, m_r$ étant premiers entre eux deux à deux.

On pourra, pour engendrer le groupe, prendre r opérations, savoir : l'une quelconque des $\varphi(m_1)$ opérations d'ordre m_1, l'une quelconque des $\varphi(m_2)$ opérations d'ordre m_2, ..., l'une quelconque des $\varphi(m_r)$ opérations d'ordre m_r.

6. *Remarque.* — Soit

$$A = \begin{vmatrix} 1 & a & a^2 & \dots & a^{n-1} \\ a^{n-1} & 1 & a & \dots & a^{n-2} \\ a^{n-2} & a^{n-1} & 1 & \dots & a^{n-3} \\ \dots & \dots & \cdot & \dots & \dots \\ a & a^2 & a^3 & \dots & 1 \end{vmatrix}.$$

Alors

$$A a^{\frac{n(n-1)}{2}} = \begin{vmatrix} 1 & a & a^2 & \dots & a^{n-1} \\ a^n & a & a^2 & \dots & a^{n-1} \\ a^n & a^{n+1} & a^2 & \dots & a^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ a^n & a^{n+1} & a^{n+2} & \dots & a^{n-1} \end{vmatrix},$$

ou

$$A a^{\frac{n(n-1)}{2}} = \begin{vmatrix} 1 & a & a^2 & \dots & a^{n-1} \\ a^n - 1 & 0 & 0 & \dots & 0 \\ a^n - 1 & a^{n+1} - a & 0 & \dots & 0 \\ \dots & \dots & \cdot & \dots & \cdot \\ a^n - 1 & a^{n+1} - a & a^{n+2} - a^2 & \dots & 0 \end{vmatrix},$$

ou

$$A a^{\frac{n(n-1)}{2}} = (-1)^{n-1} a^{n-1} (a^n - 1)(a^{n+1} - a)(a^{n+2} - a^2) \dots (a^{2n-2} - a^{n-2}).$$

$$A = (-1)^{n-1} (a^n - 1)^{n-1}.$$

Bref,

$$A = (1 - a^n)^{n-1}.$$

7. *Cas particulier :* G_{p^2}. — Ici le groupe sera nécessairement engendré par une seule opération, a, d'ordre p^2. On a

$$a^{p^2} = 1,$$

comme unique équation de définition.

Le groupe régulier correspondant sera engendré par l'opération $(1, 2, 3, \ldots, p^2)$.

Les opérations sont a^λ (l'exposant λ est pris suivant le module p^2).

a^λ est d'ordre p^2 si λ est premier avec p : cela donne

$$\varphi(p^2) = p(p-1)$$

opérations d'ordre p^2.

On a

$$\varphi(p) = p - 1$$

opérations d'ordre p, savoir : $a^{\lambda p}$ (λ premier avec p).

Il y a trois sous-groupes : l'un est composé de l'opération identique; l'autre est d'ordre p, c'est $\{a^p\}$. Le troisième est le groupe donné $\{a\}$.

Chaque opération est conjuguée d'elle-même, chaque sous-groupe est conjugué de lui-même.

Le groupe des isomorphismes est un groupe cyclique d'ordre $p(p-1)$, $(G_{p(p-1)})$. Il est composé des isomorphismes

$$A_\alpha = \begin{pmatrix} a^x \\ a^{\alpha x} \end{pmatrix} \qquad (\alpha \text{ premier avec } p).$$

Si α appartient à l'exposant $p(p-1) \pmod{p^2}$, A_α engendrera tout le groupe des isomorphismes.

Remarque. — Soit

$$B = [1, a^p, a^{2p}, \ldots, a^{(p-1)p}]$$

et

$$A = aB = [a, a^{1+p}, a^{1+2p}, \ldots, a^{1+(p-1)p}];$$

alors

$$A^\alpha = a^\alpha B^\alpha = a^\alpha B = [a^\alpha, a^{\alpha+p}, \ldots, a^{\alpha+(p-1)p}].$$

En particulier,

$$A^p = B$$

(A étant un ensemble d'opérations, B un autre ensemble d'opérations; AB est l'ensemble des opérations distinctes

obtenues en multipliant une opération de A par une opération de B).

(Si A est un groupe, on a $A^2 = A$.)

8. *Groupe* $(G_p)^2$. — Les équations de définition sont

$$a^p = b^p = 1, \qquad ab = ba.$$

Il y a deux opérations génératrices, a et b, toutes deux d'ordre p.

Il est impossible de concevoir que le groupe soit engendré autrement.

Le groupe régulier de substitutions isomorphe à $(G_p)^2$ sera engendré par les deux substitutions

$$a = \prod_{h=1}^{p} (x_{h1} x_{h2} \ldots x_{hp}),$$

$$b = \prod_{k=1}^{p} (x_{1k} x_{2k} \ldots x_{pk})$$

ou

$$a^\alpha = \begin{pmatrix} h & k \\ h+\alpha & k \end{pmatrix}, \qquad b^\beta = \begin{pmatrix} h & k \\ h & k+\beta \end{pmatrix},$$

$$a^\alpha b^\beta = \begin{pmatrix} h & k \\ h+\alpha & k+\beta \end{pmatrix}$$

[h et k étant pris (mod p)].

Toutes les opérations sont d'ordre p (sauf l'opération identique).

Il y a donc $p^2 - 1$ opérations d'ordre p.

Posons

$$A_h = \begin{vmatrix} a_{1h} & a_{2h} & \ldots & a_{ph} \\ a_{ph} & a_{1h} & \ldots & a_{p-1,h} \\ \ldots & \ldots & \ldots & \ldots\ldots \\ a_{2h} & a_{3h} & \ldots & a_{1h} \end{vmatrix},$$

$$a_{11} = 1, \qquad a_{21} = a, \qquad a_{31} = a^2, \qquad \ldots, \qquad a_{p1} = a^{p-1},$$

$$a_{ij} = a^{i-1} b^{j-1}.$$

La Table de multiplication sera

$$\begin{vmatrix} A_1 & A_2 & \dots & A_p \\ A_p & A_1 & \dots & A_{p-1} \\ \dots & \dots & \dots & \dots \\ A_2 & A_3 & \dots & A_1 \end{vmatrix}.$$

A_1 représente le groupe $\{a\}$:

$$A_h = \{a\} b^{h-1}, \qquad A_h^p = \{a\}, \qquad A_h^\alpha = \{a\} b^{\alpha(h-1)}.$$

Si l'on a

$$\alpha(h-1) = k-1 \qquad (\text{mod}\, p),$$

$$A_h^\alpha = A_k;$$

donc

$$A_h^\alpha = A_{1+\alpha(h-1)}.$$

9. Loi de multiplication :

$$a^x b^y a^\lambda b^\mu = a^{x+\lambda} b^{y+\mu}.$$

D'où

$$a^\lambda b^\mu = \begin{pmatrix} a^x & b^y \\ a^{x+\lambda} & b^{y+\mu} \end{pmatrix};$$

x et y sont des nombres entiers pris suivant le module p.

10. Nous avons dit qu'il y avait $p^2 - p$ opérations d'ordre p.

Chaque groupe cyclique d'ordre p en contient $(p-1)$.

Il en résulte qu'il y a $p+1$ sous-groupes cycliques d'ordre p, savoir :

$$\{a\}, \quad \{b\}, \quad \{ab\}, \quad \{a^2 b\}, \quad \dots, \quad \{a^{p-1} b\}.$$

En comptant l'opération identique G_1 et le groupe $(G_p)^2$, cela fait $p+3$ groupes, en tout.

Toute opération est conjuguée d'elle-même.

Tout sous-groupe est conjugué de lui-même.

11. *Étude du groupe des isomorphismes de* $(G_p)^2$. — Le

groupe des isomorphismes de $(G_p)^2$ est simplement isomorphe avec le groupe G formé des substitutions $|\alpha x + \beta y, \gamma x + \delta y|$ où α, β, γ, δ sont des entiers pris suivant le module p, avec l'unique condition que $\alpha\delta - \beta\gamma$ soit incongru à zéro (mod p).

On peut avoir l'ordre du groupe G comme il suit :

Soient a et b deux opérations génératrices du groupe $(G_p)^2$. On obtiendra tous les isomorphismes de $(G_p)^2$ en remplaçant a par l'une quelconque des $p^2 - 1$ opérations d'ordre p de $(G_p)^2$. Soit a' l'opération choisie; il faudra ensuite remplacer b par l'une quelconque des $p^2 - p$ opérations d'ordre p n'appartenant pas au groupe $\{a'\}$.

Il y a donc en tout $(p^2 - 1)(p^2 - p)$ isomorphismes.

12. Considérons la substitution $|\alpha x + \beta y, \gamma x + \delta y|$.

L'isomorphisme correspondant transforme $a^x b^y$ en

$$a^{\alpha x + \beta y} b^{\gamma x + \delta y}.$$

Nous pouvons chercher les sous-groupes d'ordre p tel que l'isomorphisme transforme chacun d'eux en lui-même.

Cela revient à résoudre les congruences simultanées

$$\left.\begin{aligned} \alpha x + \beta y &\equiv \sigma x \\ \gamma x + \delta y &\equiv \sigma y \end{aligned}\right\} \quad (\text{mod } p).$$

σ doit être racine de la congruence

$$\Delta(\sigma) = \begin{vmatrix} \alpha - \sigma & \beta \\ \gamma & \delta - \sigma \end{vmatrix} \equiv 0 \qquad (\text{mod } p).$$

Nous avons quatre cas à considérer.

13. *Premier cas.* — Tous les premiers mineurs du déterminant $\Delta(\sigma)$ sont nuls. Ceci donne

$$\sigma \equiv \alpha \equiv \delta, \qquad \beta \equiv \gamma \equiv 0.$$

Les substitutions correspondantes $|\alpha x, \alpha y|$ sont dites substitutions *singulières*.

Si l'on suppose que α appartient à l'exposant $p-1$ (mod p), la substitution $|\alpha x, \alpha y|$ est d'ordre $p-1$; elle engendre le groupe des substitutions singulières, groupe cyclique d'ordre $p-1$.

14. Il est aisé de voir que toute substitution singulière est conjuguée d'elle-même dans le groupe G.

Soit d'ailleurs

$$t = |ax + by, cx + dy|,$$
$$s = |\alpha x + \beta y, \gamma x + \delta y|.$$

Écrivons qu'on a $st = ts$, quelle que soit la substitution t :

$$st = |a(\alpha x + \beta y) + b(\gamma x + \delta y), c(\alpha x + \beta y) + d(\gamma x + \delta y)|,$$
$$ts = |\alpha(ax + by) + \beta(cx + dy), \gamma(ax + by) + \delta(cx + dy)|.$$

On a donc

$$\left.\begin{aligned} a\alpha + b\gamma &\equiv \alpha a + \beta c \\ a\beta + b\delta &\equiv \alpha b + \beta d \\ c\alpha + d\gamma &\equiv \gamma a + \delta c \\ c\beta + d\gamma &\equiv \gamma a + \delta d \end{aligned}\right\} \pmod{p}.$$

Ces congruences devant être vérifiées quels que soient a, b, c, d, on a

$$\beta \equiv 0, \qquad \gamma \equiv 0, \qquad \alpha \equiv \delta \qquad \pmod{p}.$$

On voit donc que le groupe des substitutions singulières est aussi le groupe des substitutions conjuguées d'elles-mêmes.

15. *Deuxième cas.* — La congruence $\Delta(\sigma) \equiv 0 \pmod{p}$ admet deux racines distinctes.

Il existe deux sous-groupes $\{a\}$, $\{b\}$, que l'isomorphisme correspondant transforme chacun en lui-même.

Cet isomorphisme est donc le suivant :

$$\begin{pmatrix} a & b \\ a^{\alpha} & b^{\beta} \end{pmatrix}.$$

Il remplace $a^x b^y$ par $a^{\alpha x} b^{\beta y}$.

La substitution correspondante est donc $(\alpha x, \beta y)$.

Il y a $(p-1)^2$ substitutions $(\alpha x, \beta y)$. Parmi elles figurent les $p-1$ substitutions singulières.

Ces $(p-1)^2$ substitutions $(\alpha x, \beta y)$ constituent un sous-groupe H de G.

Soit K le groupe des substitutions singulières : $\frac{H}{K}$ est d'ordre $p-1$.

D'ailleurs $(\alpha x, \beta y) = (\alpha x, \alpha y)\left(x, \frac{\beta}{\alpha} y\right)$.

Prenons pour $\frac{\beta}{\alpha}$ un nombre appartenant à l'exposant $p-1 \pmod p$; on voit que le groupe $\frac{H}{K}$ est cyclique.

16. Comme il y a $p+1$ sous-groupes d'ordre p et qu'on peut choisir arbitrairement les deux sous-groupes que l'isomorphisme transformera chacun en lui-même, on aura donc $\frac{1}{2} p(p+1)$ sous-groupes H, d'ordre $(p-1)^2$, contenant le groupe K des substitutions singulières.

17. Soit

$$\begin{aligned} s &= (\alpha x, \beta y), \\ s' &= (\alpha' x, \beta' y), \\ t &= (ax + by, cx + dy). \end{aligned}$$

Écrivons qu'on a $st = ts'$:

$$\begin{aligned} st &= (a\,\alpha x + b\,\beta y, c\,\alpha x + d\,\beta y), \\ ts' &= (\alpha' ax + \alpha' by, \beta' cx + \beta' dy); \end{aligned}$$

d'où

$$\left.\begin{aligned} a(\alpha - \alpha') &\equiv 0, \qquad b(\alpha' - \beta) \equiv 0 \\ c(\alpha - \beta') &\equiv 0, \qquad d(\beta - \beta') \equiv 0 \end{aligned}\right\} \pmod p.$$

On peut donc, ou bien supposer

$$b \equiv c \equiv 0, \qquad \alpha \equiv \alpha', \qquad \beta \equiv \beta' \qquad (\text{mod } p);$$

alors $t = (ax, dy)$ fait partie du groupe H; ou bien faire

$$a \equiv d \equiv 0, \qquad \alpha \equiv \beta', \qquad \alpha' \equiv \beta \qquad (\text{mod } p);$$

alors

$$t = (by, ax).$$

Mais $t^2 = (abx, aby)$ est une substitution singulière.

Le groupe $\{H, t\}$ est donc d'ordre $2(p-1)^2$.

Le nombre des groupes H conjugués les uns des autres dans le groupe G est donc

$$\frac{(p^2-1)(p^2-p)}{2(p-1)^2} = \frac{1}{2}p(p+1).$$

Or, il y a précisément $\frac{1}{2}p(p+1)$ sous-groupes H.

Donc : les $\frac{1}{2}p(p+1)$ sous-groupes H forment une suite complète unique de sous-groupes conjugués.

Chaque groupe donne $(p-1)^2 - (p-1) = (p-1)(p-2)$ substitutions non singulières. Donc, en tout, nous aurons ainsi

$$\frac{1}{2}p(p+1)(p-1)(p-2)$$

substitutions non encore énumérées.

18. *Troisième cas.* — La congruence $\Delta(\sigma) = 0$ a une racine double, mais tous les mineurs du déterminant $\Delta(\sigma)$ ne sont pas nuls.

On a

$$(\alpha + \delta)^2 \equiv 4(\alpha\delta - \beta\gamma) \qquad (\text{mod } p).$$

L'isomorphisme correspondant transforme en lui-même un seul sous-groupe d'ordre p.

Soit $\{a\}$ ce sous-groupe.

L'isomorphisme sera de la forme

$$\begin{pmatrix} a & b \\ a^{\alpha}, & a^{\beta} b^{\delta} \end{pmatrix}.$$

Il transforme $a^x b^y$ en $a^{\alpha x+\beta y} b^{\delta y}$.

La substitution correspondante est donc $(\alpha x + \beta y, \delta y)$.

Les substitutions de cette forme constituent un groupe, car on a

$$\begin{aligned}(\alpha x + \beta y, \delta y)(\alpha' x + \beta' y, \delta' y) &= [\alpha'(\alpha x + \beta y) + \beta' \delta y, \delta' \delta y], \\ &= [\alpha\alpha' x + (\beta\alpha' + \delta\beta') y, \delta' \delta y].\end{aligned}$$

Dans ce groupe, les substitutions cherchées sont celles pour lesquelles on a

$$(\alpha + \delta)^2 \equiv 4\alpha\delta \qquad \text{ou} \qquad \alpha \equiv \delta \qquad (\text{mod } p).$$

Ce sont donc les substitutions $(\alpha x + \beta y, \alpha y)$.

α peut prendre les valeurs $1, 2, \ldots, p-1$; β les valeurs $0, 1, 2, \ldots, p-1$. Elles sont donc en nombre $p(p-1)$. Elles contiennent les substitutions singulières.

19. Soit

$$\begin{aligned} s &= (\alpha x + \beta y, \alpha y), \\ s^2 &= (\alpha^2 x + \alpha\beta y + \beta\alpha y, \alpha^2 y) = (\alpha^2 x + 2\alpha\beta y, \alpha^2 y), \\ s^3 &= [\alpha^2(\alpha x + \beta y) + 2\alpha^2\beta y, \alpha^3 y] = (\alpha^3 x + 3\alpha^2\beta y, \alpha^3 y). \end{aligned}$$

D'une façon générale,

$$s^{\mu} = (\alpha^{\mu} x + \mu\alpha^{\mu-1}\beta y, \alpha^{\mu} y).$$

S'il ne s'agit pas d'une substitution singulière, c'est-à-dire si l'on suppose $\beta \neq 0$, comme $s^p = (\alpha x, \alpha y)$, s^p est la première puissance de s qui fasse partie du groupe K des substitutions singulières.

20. Les substitutions $(\alpha x + \beta y, \alpha y)$ forment un groupe I contenant le groupe K.

On a

$$(\alpha x+\beta y, ay)(ax+by, cx+dy)=\begin{pmatrix} a\alpha x+a\beta y & c\alpha x+c\beta y \\ +b\alpha y & +d\alpha y \end{pmatrix},$$

$$(ax+by, cx+dy)(\alpha' x+\beta' y, \alpha' y)=\begin{pmatrix} \alpha' ax+\alpha' by & \alpha' cx+\alpha' dy \\ +\beta' cx+\beta' dy & \end{pmatrix}.$$

Donc, pour qu'une substitution $t=(ax+by,\ cx+dy)$ soit permutable avec le groupe I, il faut

$$\left.\begin{aligned} a\alpha &\equiv a\alpha'+c\beta' \\ a\beta+b\alpha &\equiv b\alpha'+d\beta' \\ c\alpha &\equiv c\alpha' \\ c\beta+d\alpha &\equiv d\alpha' \end{aligned}\right\} \pmod p.$$

L'hypothèse $c\not\equiv 0$ entraîne $\alpha'\equiv\alpha$, $\beta\equiv 0$, $\beta'\equiv 0$; la substitution t n'est donc permutable qu'avec le groupe K des substitutions singulières.

Donc il faut qu'on ait $c\equiv 0$.

Les congruences précédentes deviennent

$$\begin{aligned} a(\alpha-\alpha') &\equiv 0, \\ a\beta+b(\alpha-\alpha') &\equiv d\beta', \\ d(\alpha-\alpha') &\equiv 0. \end{aligned}$$

On a, nécessairement, $ad\not\equiv 0$.

Donc

$$\alpha\equiv\alpha', \qquad d\beta'\equiv\alpha\beta \qquad \pmod p.$$

Ainsi les substitutions $(ax+by, dy)$ sont permutables avec le groupe I.

Elles sont en nombre $p(p-1)^2$, puisque b peut prendre toutes les valeurs entières (mod p), tandis que a et d sont simplement assujettis l'un et l'autre à n'être pas nuls (mod p).

Le nombre des groupes I transformés les uns des autres est donc

$$\frac{(p^2-1)(p^2-p)}{p(p-1)^2}=\frac{p(p-1)^2(p+1)}{p(p-1)^2}=p+1.$$

Or, il y a justement $p+1$ sous-groupes I, car chacun d'eux est caractérisé par ce fait qu'un des $p+1$ sous-groupes d'ordre p de $(G_p)^2$ est transformé en lui-même.

Donc les $p+1$ sous-groupes I, d'ordre $p(p-1)$, qui contiennent tous le groupe K des substitutions singulières, forment une suite complète unique de sous-groupes conjugués.

Chaque sous-groupe I donne $p(p-1)-(p-1)=(p-1)^2$ substitutions non encore énumérées, ce qui donne un total de $(p+1)(p-1)^2$ substitutions non encore énumérées.

21. *Quatrième cas.* — Restent enfin les substitutions telles que la congruence caractéristique

$$\Delta(\sigma) \equiv \begin{vmatrix} \alpha-\sigma & \beta \\ \gamma & \delta-\sigma \end{vmatrix} \equiv 0 \pmod{p}$$

soit irréductible.

Nous pouvons toujours supposer que l'isomorphisme transforme le sous-groupe $\{a\}$ en le sous-groupe $\{b\}$, puis le sous-groupe $\{b\}$ en $\{a^\beta b^\delta\}$.

L'isomorphisme transforme alors

$$a^x b^y \quad \text{en} \quad b^x a^{\beta y} b^{\delta y} = a^{\beta y} b^{x+\delta y}.$$

Par suite, à l'isomorphisme répond la substitution

$$(\beta y, x+\delta y).$$

La congruence caractéristique est

$$\begin{vmatrix} -\sigma & \beta \\ 1 & \delta-\sigma \end{vmatrix} \equiv \sigma^2-\delta\sigma-\beta \equiv 0 \pmod{p}.$$

Prenons comme congruence fondamentale la congruence

$$f(x) \equiv 0 \pmod{p},$$

$f(x)$ étant un polynome du deuxième degré, à coefficients entiers, irréductible (mod p).

Soient alors j et j^p les racines imaginaires de la congruence $\Delta(\sigma) \equiv 0 \{\bmod [p, f(x)]\}$. On a

$$\delta = j + j^p, \qquad \beta = -j^{1+p}.$$

Soit d'ailleurs

$$s = (\beta y, x + \delta y) = [-j^{p+1} y, x + (j + j^p) y].$$

On a

$$s^2 = [\beta x + \beta \delta y, \delta x + (\beta + \delta^2) y],$$

ou

$$s^2 = [-j^{p+1} x - j^{p+1}(j + j^p) y, (j + j^p) x + (j^2 + j^{2p} + j^{p+1}) y],$$

ou

$$s^2 = \left(-j^{p+1} x - j^{p+1} \frac{j^2 - j^{2p}}{j - j^p} y, \frac{j^2 - j^{2p}}{j - j^p} x + \frac{j^3 - j^{3p}}{j - j^p} y\right).$$

22. Soit, d'une façon générale,

$$s^\mu = \left(-j^{p+1} \frac{j^{\mu-1} - j^{(\mu-1)p}}{j - j^p} x - j^{p+1} \frac{j^\mu - j^{\mu p}}{j - j^p} y \right.$$
$$\left. + \frac{j^\mu - j^{\mu p}}{j - j^p} x + \frac{j^{\mu+1} - j^{(\mu+1)p}}{j - j^p} y\right).$$

On aura

$$s^{\mu+1} = \left[-j^{p+1} \frac{j^\mu - j^{\mu p}}{j - j^p} x - j^{p+1} \frac{j^{\mu+1} - j^{(\mu+1)p}}{j - j^p} y, \right.$$
$$-j^{p+1} \frac{j^{\mu-1} - j^{(\mu-1)p}}{j - j^p} x - j^{p+1} \frac{j^\mu - j^{\mu p}}{j - j^p} y$$
$$\left. + (j + j^p) \frac{j^\mu - j^{\mu p}}{j - j^p} x + (j + j^p) \frac{j^{\mu+1} - j^{(\mu+1)p}}{j - j^p} y\right].$$

Mais

$$(j^\mu - j^{\mu p})(j + j^p) - j^{p+1}(j^{\mu-1} - j^{(\mu-1)p})$$
$$= j^{\mu+1} + j^{p+\mu} - j^{1+\mu p} - j^{(\mu+1)p} - j^{p+\mu} + j^{1+\mu p} = j^{\mu+1} - j^{(\mu+1)p}.$$

De sorte que la loi est générale.

23. *Faisons l'hypothèse* que j appartient à l'exposant $(p^2 - 1) \{\bmod [p, f(x)]\}$. Pour que s soit une substi-

tution singulière, il faut qu'on ait simultanément

$$\left.\begin{array}{c} j^{\mu} \equiv j^{\mu p}, \\ j^{\mu+1} - j^{(\mu+1)p} + j^{p+1}(j^{\mu-1} - j^{(\mu-1)p}) \equiv 0 \end{array}\right\} \quad \{\bmod [p, f(x)]\}.$$

La dernière congruence donne, en tenant compte de la première,

$$j^{\mu+1} - j^{p+\mu} + j^{p+\mu} - j^{1+\mu} \equiv 0;$$

elle est donc identiquement vérifiée.

Reste à vérifier la première :

$$j^{\mu}(j^{\mu(p-1)} - 1) \equiv 0 \qquad \{\bmod [p, f(x)]\}.$$

Puisqu'on suppose que j appartient à l'exposant $p^2 - 1$ $\{\bmod [p, f(x)]\}$, il en résulte que μ devra être égal à $p + 1$.

24. Cherchons, d'ailleurs, le nombre des substitutions à congruence irréductible.

Nous avons trouvé $p - 1$ substitutions singulières.

Les groupes H ont donné

$$\frac{1}{2} p(p+1)(p-1)(p-2)$$

autres substitutions, et les groupes I

$$(p+1)(p-1)^2$$

substitutions nouvelles.

Le nombre des substitutions à congruence irréductible est donc

$$\begin{aligned}
&(p^2-1)(p^2-p) - \left[p - 1 + \frac{(p-2)(p-1)p(p+1)}{2} + (p+1)(p-1)^2\right] \\
&= (p-1)\frac{1}{2}[2(p+1)(p^2-p) - 2 - p(p+1)(p-2) - 2(p^2-1)] \\
&= \frac{p-1}{2} A,
\end{aligned}$$

avec

$$A = \begin{vmatrix} 2p^3 & -2p^2 & -2p & -2 \\ & +2p^2 & & \\ -p^3 & +p^2 & +2p & \\ & -2p^2 & & +2 \end{vmatrix} = p^3 - p^2 = p^2(p-1).$$

Le nombre des substitutions à congruence irréductible est, en définitive,

$$\frac{p^2(p-1)^2}{2}.$$

25. Comptons les congruences irréductibles.

Il y a p^2 polynomes du second degré en σ tels que le coefficient de σ^2 soit égal à 1. Parmi eux il y a p polynomes carrés parfaits et $\frac{p(p-1)}{2}$ polynomes qui, égalés à zéro, ont des racines réelles et distinctes.

Restent donc $p^2 - p - \frac{p(p-1)}{2} = \frac{p(p-1)}{2}$ congruences irréductibles.

Donc à chaque congruence irréductible sont attachées $p(p-1)$ substitutions.

26. Dans le cas où j appartient à l'exposant $p^2 - 1$ $\{\bmod [p, f(x)]\}$, si l'on considère la substitution

$$s = [-j^{p+1}y,\ x + (j + j^p)y],$$

on a

$$s^{p+1} = \left(-j^{p+1}\frac{j^p - j^{p^2}}{j - j^p}x,\ \frac{j^{p+2} - j^{(p+2)p}}{j - j^p}y\right)$$

ou

$$s^{p+1} = (j^{p+1}x, j^{p+1}y).$$

Comme j^{p+1} appartient à l'exposant $p - 1$ $\{\bmod [p, f(x)]\}$, on en conclut que β appartient à l'exposant $p - 1$ (mod p).

s est donc d'ordre $p^2 - 1$.

La substitution s engendre un groupe qui contient le groupe K des substitutions singulières. Le nombre des sub-

stitutions de ce groupe autres que les substitutions singulières est

$$p^2 - 1 - (p - 1) = p(p - 1).$$

27. Soit $s = (\alpha x + \beta y, \gamma x + \delta y)$ une substitution à congruence caractéristique irréductible et supposons que, j et j^p étant les racines de cette congruence caractéristique, j appartienne à l'exposant $p^2 - 1$ $\{\bmod [p, f(x)]\}$.

Il existe deux formes linéaires, $ux + vy$, $u'x + v'y$, à coefficients imaginaires de Galois, que s transforme en $j(ux + vy)$ et $j^p(u'x + v'y)$ respectivement.

Posons

$$x' = ux + vy, \qquad y' = u'x + v'y,$$

et prenons x' et y', au lieu de x et de y, comme variables. La substitution s devient $(jx, j^p y)$.

Alors, les seules substitutions permutables avec s qui ne se réduisent pas à une puissance de s sont de la forme (by, cx) (*voir* le deuxième cas); leur carré est une substitution singulière.

Par suite, le groupe des substitutions permutables avec s est d'ordre $2(p^2 - 1)$. Le nombre des substitutions conjuguées de s est donc

$$\frac{(p^2 - 1)(p^2 - p)}{2(p - 1)} = \frac{p(p - 1)}{2}.$$

Par suite, on peut dire qu'il y a $\frac{1}{2}p(p - 1)$ sous-groupes cycliques engendrés chacun par une substitution à congruence caractéristique irréductible, substitution d'ordre $p^2 - 1$, et que ces $\frac{1}{2}p(p - 1)$ sous-groupes forment une suite complète unique de sous-groupes conjugués.

28. En résumé, le groupe G contient :

1° Le groupe K des substitutions singulières, groupe cyclique d'ordre $p - 1$.

2° $\frac{1}{2}p(p+1)$ groupes H contenant chacun le groupe K ; chaque groupe H est d'ordre $(p-1)^2$; les substitutions correspondantes sont telles que la congruence caractéristique a deux racines réelles et distinctes. Les groupes H forment une suite complète unique de sous-groupes conjugués.

3° $p+1$ sous-groupes I d'ordre $p(p-1)$ contenant chacun le groupe K. La congruence caractéristique de chaque substitution d'un tel groupe I a une racine double. Les groupes I forment une suite complète de sous-groupes conjugués.

4° Enfin, $\frac{1}{2}p(p-1)$ groupes cycliques J engendrés chacun par une substitution d'ordre p^2-1 à congruence caractéristique irréductible. Ces groupes J forment encore une suite complète unique de sous-groupes conjugués.

29. *Vérification :*

$$p-1+\frac{1}{2}p(p+1)(p-1)(p-2)+(p+1)(p-1)^2+\frac{1}{2}p^2(p-1)^2$$

$$=(p-1)\frac{1}{2}\left[2+p(p+1)(p-2)+(p^2-1)^2+p^2(p-1)\right]$$

$$=\frac{p(p-1)}{2}\left[(p+1)(p-2)+2p+p(p-1)\right]$$

$$=\frac{p(p-1)}{2}\left[(p+1)(p-2)+p(p+1)\right]$$

$$=\frac{p(p^2-1)}{2}(p-2+p)=p(p-1)(p^2-1)=(p^2-1)(p^2-p).$$

30. *Exemple :* $(G_e)^2$. — Une première manière de définir ce groupe consiste à écrire les équations de définition qui suivent :

$$a^2=b^2=1, \qquad ab=ba.$$

Le groupe contient alors quatre opérations : 1, a, b, ab.

Deux quelconques des trois opérations a, b, $ab = c$ peuvent servir d'opérations génératrices.

On a

$$ab = c, \qquad ac = b, \qquad bc = a.$$

Voici les sous-groupes : $[1]$, $[1, a]$, $[1, b]$, $[1, c]$, $[1, a, b, c]$.

31. Nous définirons ainsi qu'il suit les *opérations à exposants imaginaires de Galois.*

Considérons le groupe $(G_p)^n$, p étant un nombre premier.

Soit $f(x)$ un polynome entier, à coefficients entiers, de degré n, irréductible suivant le module p.

Choisissons la congruence $f(x) \equiv 0 \pmod{p}$ comme congruence fondamentale.

Soit j une imaginaire de Galois. j sera de la forme

$$\alpha_1 + \alpha_2 x + \alpha_3 x^2 + \ldots + \alpha_n x^{n-1},$$

$\alpha_1, \alpha_2, \ldots, \alpha_n$ étant des nombres entiers pris suivant le module p.

Le groupe $(G_p)^n$ est engendré par n opérations distinctes d'ordre p que je désignerai par $a_1, a_2, \ldots, a_n$.

Je considère une opération unique a.

Je définis a^j par la formule $a^j = a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}$.

De cette façon, toutes les opérations du groupe seront représentées par les puissances, réelles ou imaginaires, de a.

On écrira, pour avertir que l'opération est susceptible d'exposants imaginaires, et pour indiquer en même temps son ordre p^n et la congruence $f(x) \equiv 0 \pmod{p}$ qui sert de congruence fondamentale,

$$a^{[p, f(x)]} = 1.$$

Si i et j sont deux imaginaires de Galois $(a^i)^j = a^{ij}$, par définition.

Exemple : $(G_2)^2$. — Prenons comme congruence fondamentale

$$x^2 + x + 1 \equiv 0 \pmod{2}.$$

Le groupe $(G_2)^2$ pourra être défini par l'équation unique

$$a^{(2,\, x^2+x+1)} = 1;$$

soit x une racine de la congruence $x^2 + x + 1 \equiv 0 \pmod 2$.

Les quatre nombres de Galois sont 0, 1, x, $1 + x$,

$$a^0 = 1, \qquad a = a_1, \qquad a^x = a_2, \qquad a^{x^2} = a^{x+1} = a_1 a_2,$$
$$x^3 \equiv x^2 + x \equiv 1, \qquad a^{x^3} = a_1.$$

32. *Groupe* G^1_{pq}. — p et q sont deux nombres premiers ($p > q$), q divise $p - 1$, α est un nombre appartenant à l'exposant $q \pmod p$.

Les équations de définition sont

$$a^p = b^q = 1, \qquad ab = ba^\alpha.$$

On a

$$ab = ba^\alpha.$$

Donc

$$a^2 b = a\, ab = a\, ba^\alpha = b\, a^{2\alpha}, \qquad \ldots,$$
$$a^\lambda b = ba^{\lambda\alpha} \qquad (\lambda \text{ entier et positif}).$$

Soit α' l'associé de $\alpha \pmod p$.

Faisons

$$\lambda = \alpha', \qquad a^{\alpha'} b = ba^{\alpha\alpha'} = ba$$

et

$$a^{\alpha'\lambda} b = ba^\lambda.$$

D'autre part,

$$ab^2 = ba^\alpha b = b^2 a^{\alpha^2}$$

et, plus généralement,

$$ab^y = b^y a^{\alpha^y}.$$

Donc

$$a^{\lambda\alpha^y} b^y = b^y a^\lambda.$$

Alors

$$a^x b^y a^\lambda b^\mu = a^x\, a^{\lambda\alpha^y} b^y\, b^\mu = a^{x+\lambda\alpha^y} b^{y+\mu}.$$

Telle est la loi de multiplication. En posant $\alpha' = \frac{1}{\alpha}$, on

pourra représenter le groupe par le symbole

$$a^\lambda b^\mu = \left| \begin{matrix} a^x b^y \\ a^{x+\lambda\alpha^{-y}} b^{y+\mu} \end{matrix} \right| = (x + \lambda\alpha^{-y},\ y + \mu)$$

$$(x = 0, 1, 2, \ldots, p-1;\ y = 0, 1, 2, \ldots, q-1).$$

33. *Opérations d'ordre donné.* — On a

$$a^x b^y = b^y a^{x\alpha^y}.$$

Donc

$$(a^x b^y)^2 = a^x b^{2y} a^{x\alpha^y}.$$

Mais

$$a^x b^{2y} = b^{2y} a^{x\alpha^{2y}}.$$

Donc

$$(a^x b^y)^2 = b^{2y} a^{x(\alpha^y + \alpha^{2y})}.$$

D'une façon générale,

$$(a^x b^y)^\lambda = b^{\lambda y} a^{x(\alpha^y + \alpha^{2y} + \ldots + \alpha^{\lambda y})}$$

ou

$$(a^x b^y)^\lambda = b^{\lambda y} a^{x\alpha^y \frac{\alpha^{\lambda y} - 1}{\alpha^y - 1}}.$$

Supposons y premier avec q. Alors α^y est différent de 1. Si l'on fait $\lambda = q$, $\alpha^{qy} - 1$ est nul (mod p). Donc on a

$$(a^x b^y)^q = 1 \ (y \text{ premier avec } q).$$

On a donc

$$\varphi(p) = p - 1 \text{ opérations d'ordre } p \ (a^x,\ x \text{ premier avec } p)$$

et

$$p\varphi(q) = p(q-1) \text{ opérations d'ordre } q \ (a^x b^y,\ y \text{ premier avec } q).$$

Il y a un seul sous-groupe cyclique d'ordre p, $\{a\}$, et p sous-groupes cycliques d'ordre q

$$\{a^x b\} \ (x = 0, 1, 2, \ldots, p-1).$$

34. *Changement d'opérations génératrices.* — Posons

$$\left.\begin{matrix} a^\lambda b^\mu = a' \\ a^\rho b^\sigma = b' \end{matrix}\right\} (\mu\sigma \neq 0)$$

et cherchons à résoudre ces équations par rapport à a et à b.

On a

$$a'^x = (a^\lambda b^\mu)^x = b^{\mu x} a^{\lambda \alpha^\mu \frac{\alpha^{\mu x}-1}{\alpha^\mu - 1}} = a^{\lambda \alpha^{\mu(1-x)} \frac{\alpha^{\mu x}-1}{\alpha^\mu - 1}} b^{\mu x},$$

$$b'^y = (a^\rho b^\sigma)^y = b^{\sigma y} a^{\rho \alpha^\sigma \frac{\alpha^{\sigma y}-1}{\alpha^\sigma - 1}} = a^{\rho \alpha^{\sigma(1-y)} \frac{\alpha^{\sigma y}-1}{\alpha^\sigma - 1}} b^{\sigma y}.$$

Donc

$$a'^x b'^y = a^{\lambda \alpha^{\mu(1-x)} \frac{\alpha^{\mu x}-1}{\alpha^\mu - 1}} b^{\mu x} a^{\rho \alpha^{\sigma(1-y)} \frac{\alpha^{\sigma y}-1}{\alpha^\sigma - 1}} b^{\sigma y}$$

ou bien

$$a'^x b'^y = a^{\lambda \alpha^{\mu(1-x)} \frac{\alpha^{\mu x}-1}{\alpha^\mu - 1} + \rho \alpha^{\sigma(1-y)} - \mu x \frac{\alpha^{\sigma y}-1}{\alpha^\sigma - 1}} b^{\mu x + \sigma y}.$$

Soit d'abord $\mu x + \sigma y \equiv 0 \pmod q$.

L'exposant de a devient

$$\lambda \alpha^{\mu(1-x)} \frac{\alpha^{\mu x} - 1}{\alpha^\mu - 1} + \rho \alpha^\sigma \frac{\alpha^{-\mu x} - 1}{\alpha^\sigma - 1}$$

ou

$$\frac{\lambda \alpha^\mu}{\alpha^\mu - 1}(1 - \alpha^{-\mu x}) - \rho \frac{\alpha^\sigma}{\alpha^\sigma - 1}(1 - \alpha^{-\mu x})$$
$$= \left(\frac{\lambda \alpha^\mu}{\alpha^\mu - 1} - \frac{\rho \alpha^\sigma}{\alpha^\sigma - 1}\right)(1 - \alpha^{-\mu x}).$$

55. Posons

$$u = \frac{\lambda \alpha^\mu}{\alpha^\mu - 1} - \frac{\rho \alpha^\sigma}{\alpha^\sigma - 1}.$$

Je dis que u est incongru à zéro $\pmod p$, si b' n'est pas une puissance de a'.

En effet,

$$a'^x = a^{\frac{\lambda \alpha^\mu}{\alpha^\mu - 1}(1 - \alpha^{-\mu x})} b^{\mu x}, \qquad b' = a^\rho b^\sigma.$$

On ne doit pas pouvoir déterminer x de façon qu'on ait simultanément

$$\mu x \equiv \sigma \pmod q$$

et

$$\rho \equiv \frac{\lambda \alpha^\mu}{\alpha^\mu - 1}(1 - \alpha^{-\mu x}) \pmod p.$$

Autrement dit, on a

$$\rho \not\equiv \frac{\lambda\alpha^{\mu}}{\alpha^{\mu}-1}(1-\alpha^{-\sigma}) \qquad (\bmod p),$$

ou

$$\rho \not\equiv \frac{\lambda\alpha^{\mu}(\alpha^{\sigma}-1)}{\alpha^{\sigma}(\alpha^{\mu}-1)} \qquad (\bmod p),$$

ou

$$\frac{\rho\alpha^{\sigma}}{\alpha^{\sigma}-1} \not\equiv \frac{\lambda\alpha^{\mu}}{\alpha^{\mu}-1} \qquad (\bmod p).$$

36. Ainsi

$$a'^{x} b'^{-\frac{\mu x}{\sigma}} = a^{u(1-\alpha^{-\mu x})}.$$

Soit z un nombre tel que $uz(1-\alpha^{-\mu x}) \equiv 1 \pmod p$ [on pourra se donner $x \not\equiv 0 \pmod q$), alors z est déterminé].

On aura

$$a = \left(a'^{x} b'^{-\frac{\mu x}{\sigma}}\right)^{z}.$$

On donnera à x les valeurs $1, 2, \ldots, q-1$, successivement z prendra les valeurs $z_1, z_2, \ldots, z_{q-1}$.

On choisira la plus petite (ou l'une des plus petites).

Ainsi, on a

$$a = \left(a'^{x} b'^{-\frac{\mu x}{\sigma}}\right)^{\frac{1}{u(1-\alpha^{-\mu x})}},$$

$\frac{1}{u(1-\alpha^{-\mu x})}$ étant pris $(\bmod p)$.

Ayant a,

$$b^{\mu} = \alpha^{-\lambda} a'.$$

Soit $\mu'\mu \equiv 1 \pmod q$,

$$b = (a^{-\lambda} a')^{\mu'}.$$

En particulier, soit

$$ab^{-1} = a', \qquad b = b',$$

d'où

$$a = a'b', \qquad b = b'.$$

On a

$$a'^q = b'^q = 1, \qquad (a'b')^p = 1.$$

Comme $ab = ba^\alpha$,

$$a'b'^2 = b'(a'b')^\alpha.$$

37. *Groupe des isomorphismes cogrédients de* G^1_{pq}. — On a

$$ab = ba^\alpha, \qquad ab^\mu = b^\mu a^{\alpha^\mu}, \qquad a^\lambda b^\mu = b^\mu a^{\lambda\alpha^\mu}, \qquad a^{\alpha-\mu} b^\mu = b^\mu a.$$

Donc

$$a^\lambda b^\mu a = a\, a^{\lambda+\alpha-\mu-1} b^\mu.$$

Bref,

$$\bar{a} = \begin{vmatrix} a^\lambda b^\mu \\ a^{\lambda+\alpha-\mu-1} b^\mu \end{vmatrix}.$$

Puis

$$a^\lambda b^\mu b = a^\lambda b^{\mu+1} = b\, a^{\lambda\alpha} b^\mu.$$

Donc

$$\bar{b} = \begin{vmatrix} a^\lambda\ b^\mu \\ a^{\lambda\alpha} b^\mu \end{vmatrix}.$$

On peut écrire ces substitutions d'une manière plus explicite, en mettant les cycles en évidence. On a d'abord

$$\bar{a} = \prod_{h=1}^{q-1} (b^h, a^{\alpha-h-1} b^h, a^{2(\alpha-h-1)} b^h, \ldots, a^{(p-1)(\alpha-h-1)} b^h).$$

Ensuite, posons

$$p = 1 + xq.$$

Les $p-1$ nombres entiers sont congrus aux $(p-1)$ nombres du Tableau :

$$\begin{array}{lllll}
\alpha_0, & \alpha_0\alpha, & \alpha_0\alpha^2, & \ldots, & \alpha_0\alpha^{q-1} \qquad \alpha_0 = 1, \\
\alpha_1, & \alpha_1\alpha, & \alpha_1\alpha^2, & \ldots, & \alpha_1\alpha^{q-1} \\
\alpha_2, & \alpha_2\alpha, & \alpha_2\alpha^2, & \ldots, & \alpha_2\alpha^{q-1} \\
\ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\
\alpha_{x-1}, & \alpha_{x-1}\alpha, & \alpha_{x-1}\alpha^2, & \ldots, & \alpha_{x-1}\alpha^{q-1}
\end{array}$$

α_i étant un nombre quelconque non congru (mod p) à aucun des nombres des i premières lignes du Tableau.

Alors on a

$$\overline{b} = \prod_{h=0}^{x-1} \prod_{k=0}^{q-1} (a^{\alpha_h} b^k,\ a^{\alpha_h \alpha} b^k,\ a^{\alpha_h \alpha^2} b^k,\ \ldots,\ a^{\alpha_h \alpha^{q-1}} b^k).$$

38. *Groupe total des isomorphismes.* — Un isomorphisme sera de la forme

$$J = \begin{vmatrix} a, & b \\ a^\lambda, & a^\mu b^\nu \end{vmatrix};$$

J transforme ab en $a^{\lambda+\mu} b^\nu$ et ba^α en $a^\mu b^\nu a^{\lambda\alpha}$.

On a donc

$$a^{\lambda+\mu} b^\nu = a^\mu b^\nu a^{\lambda\alpha}$$

ou

$$a^\lambda b^\nu = b^\nu a^{\lambda\alpha}.$$

Mais

$$a^\lambda b^\nu = b^\nu a^{\lambda\alpha^\nu}.$$

Donc on a

$$\alpha^\nu \equiv \alpha \qquad (\text{mod } p);$$

donc

$$\nu = 1.$$

Les isomorphismes sont donnés par la formule générale

$$J_{\lambda\mu} = \begin{pmatrix} a & b \\ a^\lambda & a^\mu b \end{pmatrix};$$

λ est premier avec p, μ est quelconque.

Le groupe des isomorphismes est donc d'ordre $p(p-1)$.

Le groupe des isomorphismes cogrédients est engendré par les deux isomorphismes

$$J_{1,\alpha^{-1}-1} \qquad \text{et} \qquad J_{\alpha,0}.$$

39. Voyons comment $J_{\lambda\mu}$ transforme $a^x b^y$.

Elle transforme cette opération en $a^{\lambda x}(a^\mu b)^y$.

Mais

$$(a^x b^y)^\lambda = b^{\lambda y} a^{x\alpha^y \frac{\alpha^{\lambda y}-1}{\alpha^y-1}};$$

donc

$$(a^\mu b)^y = b^y a^{\mu\alpha\frac{\alpha^y-1}{\alpha-1}} = a^{\mu\alpha\frac{1-\alpha^{-y}}{\alpha-1}} b^y;$$

donc

$$J_{\lambda\mu} = \begin{pmatrix} a^x b^y \\ a^{\lambda x + \mu\alpha\frac{1-\alpha^{-y}}{\alpha-1}} b^y \end{pmatrix},$$

$$J_{\lambda\mu} J_{\lambda'\mu'} = \begin{pmatrix} a^x b^y \\ a^{\lambda'\lambda x + \lambda'\mu\alpha\frac{1-\alpha^{-y}}{\alpha-1} + \mu'\alpha\frac{1-\alpha^{-y}}{\alpha-1}} b^y \end{pmatrix} = J_{\lambda\lambda', \lambda'\mu+\mu'},$$

$$J^k_{\lambda\mu} = J_{\lambda^k, (\lambda^{k-1}+\lambda^{k-2}+\ldots+1)\mu}.$$

Si $\lambda = 1$,

$$J^k_{1,\mu} = J_{1,k\mu}.$$

D'ailleurs $J_{1,0} = 1$; donc

$$J^p_{1,\mu} = 1 \qquad (\mu \neq 0).$$

Si $\lambda \neq 1$,

$$J^k_{\lambda,\mu} = J_{\lambda^k \frac{\lambda^k-1}{\lambda-1}\mu}.$$

Soit k l'exposant auquel appartient λ (mod p); alors $\lambda^k \equiv 1$ (mod p),

$$J^k_{\lambda\mu} = 1.$$

40. *Application à* G^1_6. — G^1_6 a pour ordre 6. Ses équations de définition sont $a^3 = b^2 = 1$, $ab = ba^2$.

Les six opérations du groupe sont 1, a, a^2, b, ab, $a^2 b$.

On a, comme sous-groupes cycliques,

$$\alpha = [1, a, a^2] \qquad \text{sous-groupe d'ordre 3,}$$

$$\left.\begin{aligned} \beta &= [1, b] \\ \beta' &= [1, ab] \\ \beta'' &= [1, a^2 b] \end{aligned}\right\} \qquad \text{sous-groupes d'ordre 2.}$$

On a

$$G = \{\alpha, \beta\} = \{\alpha, \beta'\} = \{\alpha', \beta''\} = \{\beta', \beta''\} = \{\beta'', \beta\} = \{\beta, \beta'\}.$$

Posons

$$ab = c, \qquad a = cb, \qquad (cb)^3 = 1;$$

donc

$$(bc)^3 = 1, \qquad b^2 = c^2 = 1.$$

Les équations $b^2 = c^2 = 1$, $(bc)^3 = 1$ peuvent servir d'équations de définition.

Soit

$$a^2 b = d.$$

On a

$$bc = db = cd = a^2, \quad cb = bd = dc = a, \quad b^2 = c^2 = d^2 = 1, \quad a^3 = 1,$$

$$[b, c, d]^2 = [1, a, a^2].$$

Ici

$$\begin{array}{cccccc} 1. & 2. & 3. & 5. & 6. & 4. \end{array}$$

$$\alpha = \begin{pmatrix} a^x b^y \\ a^{x+2^{-y}} b^y \end{pmatrix} = \begin{pmatrix} 1 & a & a^2 & ab & a^2 b & b \\ a & a^2 & 1 & b & ab & a^2 b \end{pmatrix},$$

$$\alpha . 2 \equiv 1 \qquad (\text{mod } 3).$$

$$\alpha = (1, 2, 3)(4, 6, 5),$$

$$b = \begin{pmatrix} a^x b^y \\ a^x b^{y+1} \end{pmatrix} = \begin{pmatrix} 1 & a & a^2 & b & ab & a^2 b \\ b & ab & a^2 b & 1 & a & a^2 \end{pmatrix},$$

$$b = (1, 4)(2, 5)(3, 6),$$

ce qui donne la Table de multiplication :

1.	a.	a^2.	b.	ab.	$a^2 b$.
1	2	3	4	5	6
3	1	2	6	4	5
2	3	1	5	6	4
4	6	5	1	3	2
5	4	6	2	1	3
6	5	4	3	2	1

Les isomorphismes cogrédients sont les suivants :

$$1, \qquad \bar{a} = (b, c, d), \qquad \bar{a}^2 = (b, d, c),$$
$$\bar{b} = (a, a^2)(c, d), \qquad \bar{c} = (a, a^2)(b, d)$$

et

$$\bar{d} = (a, a^2)(b, c).$$

C'est d'ailleurs aussi le groupe total des isomorphismes; en effet, prenons les équations de définition

$$a^3 = b^2 = 1, \qquad ab = ba^2.$$

On peut remplacer a par a ou a^2, et b par b ou c ou d. En tout 6 isomorphismes.

Autrement, soient

$$b^2 = c^2 = 1, \qquad (bc)^3 = 1$$

les équations de définition. On peut prendre pour b l'une des opérations b, c, d, soit b', puis pour c l'une des deux opérations d'ordre 2 qui restent. En tout 6 isomorphismes.

Le groupe G_6^1 n'a donc que des isomorphismes cogrédients.

Il n'y a pas d'ailleurs dans G_6^1 d'opération conjuguée d'elle-même. Ainsi G_6^1 est un groupe complet (*Burnside*, § 165, p. 236).

En considérant les sous-groupes on a

$$\bar{a} = (\beta, \beta', \beta''), \qquad \bar{a}^2 = (\beta, \beta'', \beta'),$$
$$\bar{b} = (\beta', \beta''), \qquad \bar{c} = (\beta'', \beta), \qquad \bar{d} = (\beta, \beta').$$

Le groupe G_6^1 est donc simplement isomorphe avec le groupe symétrique de trois éléments.

Les suites complètes d'opérations composées sont

$$1; \qquad a, \quad a^2; \qquad b, \quad c, \quad d.$$

Les suites complètes de sous-groupes conjugués sont

$$1; \quad \alpha; \quad \beta, \quad \beta', \quad \beta''.$$

41. Les groupes d'ordre 8 :

a. Groupe G_8 :

$$a^8 = 1.$$

Sous-groupes :

$$\{1\}, \quad \{a^4\} = \alpha, \quad \{a^2\} = \beta, \quad \{a\} = G_8.$$

Il y a 4 isomorphismes :

$$1, \quad A = (a, a^3)(a^2, a^6)(a^5, a^7),$$
$$B = (a, a^5)(a^3, a^7), \quad AB = (a, a^7)(a^2, a^6)(a^3, a^5).$$

Ces isomorphismes transforment chaque sous-groupe en lui-même.

42. *b. Groupe* G_4G_2 :

$$a^4 = b^2 = 1, \quad ab = ba.$$

Soit

$$a = a_1, \quad ab = a_2, \quad a^3 = a_3, \quad a^3 b = a_4,$$
$$b = b_1, \quad a^2 b = b_2,$$
$$a^2 = c.$$

Sous-groupes : $\{1\}$,

$$\{a\} = [a, a^2, a^3, 1] = [a_1, c, a_3, 1] = \alpha_1,$$
$$\{ab\} = [ab, a^2, a^3 b, 1] = [a_2, c, a_4, 1] = \alpha_2,$$
$$\{b\} = [1, b_1] = \beta_1,$$
$$\{a^2 b\} = [1, b_2] = \beta_2,$$
$$\{c\} = [1, a^2] = \gamma,$$
$$G_4G_2 = \{a, b\}, \quad [1, b, a^2, a^2 b] = [1, b_1, c, b_2] = \delta = \{b, a^2\}.$$

Isomorphismes. — On peut remplacer a par a, ab, a^3, $a^3 b$; b par b, $a^2 b$. En tout 8 isomorphismes.

Soit $A = \begin{pmatrix} a & b \\ ab & a^2 b \end{pmatrix}$,

$$aA = Aab, \qquad abA = Aa^3, \qquad a^3 A = Aa^3 b, \qquad a^3 bA = Aa;$$
$$bA = Aa^2 b, \qquad a^2 bA = Ab, \qquad a^2 A = Aa^2.$$

$$\begin{aligned}
A &= (a, ab, a^3, a^3 b)(b, a^2 b) = (a_1, a_2, a_3, a_4)(b_1, b_2) = (\alpha_1, \alpha_2)(\beta_1, \beta_2),\\
A^2 &= (a, a^3)(ab, a^3 b) \qquad\quad = (a_1, a_3)(a_2, a_4),\\
A^3 &= (a, a^3 b, a^3, ab)(b, a^2 b) = (a_1, a_4, a_3, a_2)(b_1, b_2) = (\alpha_1, \alpha_2)(\beta_1, \beta_2),\\
A^4 &= 1.
\end{aligned}$$

Soit $B = \begin{pmatrix} a & b \\ a^3 & a^2 b \end{pmatrix}$; donc

$$\begin{aligned}
B &= (a, a^3)(b, a^2 b) \quad = (a_1, a_3)(b_1, b_2) = (\beta_1, \beta_2),\\
AB &= (a, ab)(a^3, a^3 b) \quad = (a_1, a_2)(a_3, a_4) = (\alpha_1, \alpha_2),\\
A^2 B &= (ab, a^3 b)(b, a^2 b) = (a_2, a_4)(b_1, b_2) = (\beta_1, \beta_2),\\
A^3 B &= (a, a^3 b)(a^3, ab) \quad = (a_1, a_4)(a_2, a_3) = (\alpha_1, \alpha_2).
\end{aligned}$$

On a

$$A = \begin{pmatrix} a^x b^y \\ a^{x+2y} b^{x+y} \end{pmatrix} = (x + 2y, x + y),$$
$$B = \begin{pmatrix} a^x b^y \\ a^{3x+2y} b^y \end{pmatrix} = (3x + 2y, y),$$

$$\begin{aligned}
A^2 &= (x + 2y + 2x + 2y, 2x + 3y) = (3x, y),\\
A^3 &= (3x + 6y, x + y) = (3x + 2y, x + y),\\
A^4 &= (9x, y) = (x, y) = 1.
\end{aligned}$$

$$\begin{aligned}
AB &= (3x + 6y + 2x + 2y, x + y) = (x, x + y),\\
A^2 B &= (9x + 2y, y) = (x + 2y, y),\\
A^3 B &= (9x + 6y + 2x + 2y, x + y) = (3x, x + y).
\end{aligned}$$

43. *c. Groupe des isomorphismes de* $(G_2)^3$. — Le groupe des isomorphismes de $(G_2)^3$ est simplement isomorphe avec le groupe G formé des substitutions

$$(\alpha x + \beta y + \gamma z, \alpha' x + \beta' y + \gamma' z, \alpha'' x + \beta'' y + \gamma'' z),$$

où les coefficients sont des nombres entiers pris (mod 2) avec

l'unique condition

$$\begin{vmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{vmatrix} \not\equiv 0 \qquad (\mathrm{mod}\, 2).$$

44. *d.* G_8^1 est défini par les équations

$$a^2 = b^2 = \alpha^2 = 1, \qquad ab = ba\alpha.$$

Une opération quelconque sera désignée par la notation $a^\lambda b^\mu \alpha^\nu$; λ, μ, ν pouvant prendre les valeurs (0, 1).

Considérons le produit

$$a^x b^y \alpha^z a^\lambda b^\mu \alpha^\nu = a^x b^y a^\lambda b^\mu \alpha^{z+\nu}.$$

Mais

$$a^p b^q = b^q a^p \alpha^{pq};$$

donc

$$b^y a^\lambda = a^\lambda b^y \alpha^{\lambda y},$$

$$a^x b^y \alpha^z a^\lambda b^\mu \alpha^\nu = a^{x+\lambda} b^{y+\mu} \alpha^{z+\nu+\lambda y}.$$

Bref,

$$a^\lambda b^\mu \alpha^\nu = \begin{pmatrix} a^x b^y \alpha^z \\ a^{x+\lambda} b^{y+\mu} \alpha^{z+\nu+\lambda y} \end{pmatrix}.$$

Numérotons les substitutions comme l'indique le Tableau ci-dessous :

	x.	y.	z.
1	0	0	0
2	1	0	0
3	0	1	0
4	0	0	1
5	0	1	1
6	1	0	1
7	1	1	0
8	1	1	1

Alors

$$a = \begin{pmatrix} a^x b^y \alpha^z \\ a^{x+1} b^y \alpha^{z+y} \end{pmatrix};$$

donc

$$a = (1, 2)(3, 8)(4, 6)(5, 7),$$
$$b = \begin{pmatrix} a^x b^y \alpha^z \\ a^x b^{y+1} \alpha^z \end{pmatrix},$$
$$b = (1, 3)(2, 7)(4, 5)(6, 8).$$

D'où la Table de multiplication :

1	2	3	4	5	6	7	8
2	1	7	6	8	4	3	5
3	8	1	5	4	7	6	2
4	6	5	1	3	2	8	7
5	7	4	3	1	8	2	6
6	4	8	2	7	1	5	3
8	3	6	7	2	5	1	4
7	5	2	8	6	3	4	1

45. *Opérations d'ordre donné* (sous-groupes cycliques) :

Ordre 2 : opérations 2, 3, 4, 5, 6,
Ordre 4 : opérations 7, $(7^2 = 4)$, 8, $(8^2 = 4)$.

On peut former le Tableau suivant :

Ordre 4...			ab			$ab\alpha$
Ordre 2...	a	b	α	$a\alpha$	$b\alpha$	α

Le groupe est isomorphe au groupe des substitutions

$$1 = (x, y, z); \quad a = (x+1, y, y+z); \quad b = (x, y+1, z);$$
$$ab = (x+1, y+1, y+z), \quad \alpha = (x, y, z+1);$$
$$b\alpha = (x, y+1, z+1), \quad a\alpha = (x+1, y, y+z+1),$$
$$ab\alpha = (x+1, y+1, y+z+1), \quad \underline{\lambda\mu\nu = (x+\lambda, y+\mu, z+\nu+\lambda y)}.$$

Il y a deux opérations d'ordre 4, cinq opérations d'ordre 2.

46. Les groupes cycliques sont

$$[1, ab, \alpha, ab\alpha]; \quad [1, a]; \quad [1, b]; \quad [1, \alpha]; \quad [1, a\alpha]; \quad [1, b\alpha].$$

Les autres sous-groupes sont

$$[1, a, \alpha, a\alpha]; \quad [1, b, \alpha, b\alpha].$$

47. *Isomorphismes cogrédients :* $ba = ab\alpha$, donc

$$\bar{a} = (b, b\alpha)(ab, ab\alpha);$$

$ab = ba\alpha$, donc

$$\bar{b} = (a, a\alpha)(ab, ab\alpha),$$
$$\overline{ab} = (a, a\alpha)(b, b\alpha).$$

Suites complètes d'opérations conjuguées :

$$1; \quad \alpha; \quad a, a\alpha; \quad b, b\alpha; \quad ab, ab\alpha.$$

Suites complètes de sous-groupes conjugués :

$$1, \quad [1, \alpha]; \quad [1, \alpha, ab, ab\alpha]; \quad [1, a], \quad [1, a\alpha], \quad [1, b]; \quad [1, b\alpha];$$
$$[1, a, \alpha, a\alpha]; \quad [1, b, \alpha, b\alpha].$$

Un isomorphisme contragrédient sera

$$\bar{c} = (a, b)(a\alpha, b\alpha)(ab, ab\alpha);$$

d'où

$$\overline{ac} = (a, b, a\alpha, b\alpha),$$
$$\overline{bc} = (a, b\alpha, a\alpha, b),$$
$$\overline{abc} = (a, b\alpha)(b, a\alpha)(ab, ab\alpha).$$

Le groupe des isomorphismes est d'ordre 8.

On a

$$\begin{aligned}
\bar{a} &= \begin{pmatrix} a, & b \\ a, & b\alpha \end{pmatrix} = \begin{pmatrix} a^x b^y \alpha^z \\ a^x b^y \alpha^{y+z} \end{pmatrix} = (x, y, y+z), \\
\bar{b} &= (x, y, x+z), \\
\overline{ab} &= (x, y, x+y+z), \\
\bar{c} &= \begin{pmatrix} a, & b \\ b, & a \end{pmatrix} = \begin{pmatrix} a^x b^y \alpha^z \\ b^x a^y \alpha^z \end{pmatrix} = \begin{pmatrix} a^x b^y \alpha^z \\ a^y b^x \alpha^{xy+z} \end{pmatrix} = (y, x, xy+z), \\
\overline{ac} &= (y, x, xy+y+z), \\
\overline{bc} &= (y, x, xy+x+z), \\
\overline{abc} &= (y, x, xy+x+y+z) \qquad [x, y \text{ et } z \text{ sont pris } (\bmod 2)].
\end{aligned}$$

De l'équation

$$a^x b^y \alpha^z a^\lambda b^\mu \alpha^\nu = a^{x+\lambda} b^{y+\mu} \alpha^{z+\nu+\lambda y}$$

je déduis, si je cherche l'inverse de $a^x b^y c^z$,

$$\lambda = x, \qquad \mu = y, \qquad \nu = z + xy;$$

$a^x b^y \alpha^{z+xy}$ est l'inverse de $a^x b^y \alpha^z$ et

$$\begin{aligned}
a^{x+\lambda} b^{y+\mu} \alpha^{z+\nu+\lambda y} a^x b^y \alpha^{z+xy} &= a^\lambda b^\mu \alpha^{z+\nu+\lambda y+z+xy+xy+x\mu} \\
&= a^\lambda b^\mu \alpha^{\nu+\lambda y+\mu x}
\end{aligned}$$

est la transformée de $a^\lambda b^\mu \alpha^\nu$ par $a^x b^y \alpha^z$.

48. *Autre mode de génération.* — On a

$$2.7 = 3, \qquad 3.2 = 8, \qquad 8^2 = 4, \qquad 8^3 = 7, \qquad 7^3 = 8;$$

donc

$$a^4 = b^2 = 1, \qquad ab = ba^3,$$

$$a^\lambda b^\mu = b^\mu a^{\lambda 3^\mu}, \qquad a^{\lambda 3^\mu} b^\mu = b^\mu a^\lambda,$$

$$a^x b^y a^\lambda b^\mu = a^x a^{\lambda 3^y} b^{y+\mu} = a^{x+\lambda 3^y} b^{y+\mu},$$

$$a^\lambda b^\mu = \begin{pmatrix} a^x b^y \\ a^{x+\lambda 3^y} b^{y+\mu} \end{pmatrix} = (x + \lambda 3^y, y + \mu).$$

Numérotons les opérations comme l'indique le Tableau ci-dessous :

	x.	y.
1	0	0
2	1	0
3	2	0
4	3	0
5	0	1
6	1	1
7	2	1
8	3	1

$$a = (x + 3^y, y) = (1, 2, 3, 4)(5, 8, 7, 6).$$
$$b = (x, y + 1) \quad = (1, 5)(2, 6)(3, 7)(4, 8).$$

D'où la nouvelle Table de multiplication :

1	2	3	4	5	6	7	8
4	1	2	3	8	5	6	7
3	4	1	2	7	8	5	6
2	3	4	1	6	7	8	5
5	8	7	6	1	4	3	2
6	5	8	7	2	1	4	3
7	6	5	8	3	2	1	4
8	7	6	5	4	3	2	1

Le Tableau des opérations est le suivant :

Ordre 4...	a	a^3				
Ordre 2...	a^2	a^2	b	ab	$a^2 b$	$a^3 b$

On peut, pour compter les isomorphismes, remplacer a par a ou a^3 et b par b, ab, a^2b, a^3b, ce qui fait 8 isomorphismes, etc.

49. *Groupe* G_8^2 :

$$a^2 = b^2 = \alpha, \qquad \alpha^2 = 1, \qquad ab = ba\alpha.$$

Une opération quelconque sera de la forme

$$a^x b^y \alpha^z \qquad [x, y \text{ sont pris } (\bmod 4),\ z \text{ est pris } (\bmod 2)].$$

On a

$$a^x b^y = b^y a^x \alpha^{xy},$$

$$a^x b^y \alpha^z a^\lambda b^\mu \alpha^\nu = a^x b^y a^\lambda b^\mu \alpha^{z+\nu} = a^{x+\lambda} b^{y+\mu} \alpha^{z+\nu+\lambda y};$$

donc

	λ.	μ.	ν.
1	0	0	0
2	1	0	0
3	0	1	0
4	0	0	1
5	0	1	1
6	1	0	1
7	1	1	0
8	1	1	1

$$a^\lambda b^\mu \alpha^\nu = \begin{pmatrix} a^x b^y \alpha^z \\ a^{x+\lambda} b^{y+\mu} \alpha^{z+\nu+\lambda y} \end{pmatrix} = (x+\lambda,\ y+\mu,\ z+\nu+\lambda y).$$

$$a = (x+1,\ y,\ z+y),$$

$$a = (1, 2, 4, 6)(3, 8, 5, 7),$$

$$b = (x,\ y+1,\ z),$$

$$b = (1, 3, 4, 5)(2, 7, 6, 8).$$

D'où la Table de multiplication :

1	2	3	4	5	6	7	8
6	1	8	2	7	4	3	5
5	7	1	3	4	8	6	2
4	6	5	1	3	2	8	7
3	8	4	5	1	7	2	6
2	4	7	6	8	1	5	3
8	5	2	7	6	3	1	4
7	3	6	8	2	5	4	1

On a

$$(a^\lambda b^\mu \alpha^\nu)^2 = a^{2\lambda} b^{2\mu} \alpha^{2\nu+\lambda\mu} = \alpha^{\lambda+\mu+\lambda\mu};$$

pour

λ.	μ.	ν.	$(a^\lambda b^\mu \alpha^\nu)^2 =$
0	0	0	1
1	0	0	α
0	1	0	α
0	0	1	1
0	1	1	α
1	0	1	α
1	1	0	α
1	1	1	α

D'où le Tableau des opérations :

Ordre 4...	a	$a\alpha$	b	$b\alpha$	ab	$ab\alpha$
Ordre 2...	α	α	α	α	α	α

50. Pour avoir les isomorphismes, on voit qu'on peut remplacer a par l'une des six opérations a, $a\alpha$, b, $b\alpha$, ab, $ab\alpha$, soit a', et b par l'une des quatre opérations qui restent dans cette suite lorsqu'on a supprimé a' et $a'\alpha$.

Soient

$$\overline{a} = (b, b\alpha)(ab, ab\alpha) = \begin{bmatrix} a^x b^y \alpha^z \\ a^x b^y \alpha^{y+z} \end{bmatrix} = (x, y, y+z),$$

$$\overline{b} = (a, a\alpha)(ab, \alpha b\alpha) = \begin{bmatrix} a^x b^y \alpha^z \\ a^x b^y \alpha^{x+z} \end{bmatrix} = (x, y, x+z);$$

$$\overline{ab} = (x, y, x+y+z),$$

$$\overline{c} = (a, a\alpha)(b, ab)(b\alpha, ab\alpha) = \begin{bmatrix} a^x b^y \alpha^z \\ a^x (ab)^y \alpha^{x+z} \end{bmatrix},$$

$$(ab)^1 = ab, \qquad (ab)^2 = \alpha, \qquad (ab)^3 = ab\alpha, \qquad (ab)^4 = 1,$$

$$(ab)^y = a^y b^y \alpha^z;$$

$z' = \varphi(y)$; pour $y = 1$, $z' \equiv 0$; pour $y = 2$, $z' \equiv 1$; pour $y = 3$, $z' \equiv 1$; pour $y = 4$, $z' \equiv 0$;

$$z' = \tfrac{1}{2} y(y-1),$$

$$(ab)^y = a^y b^y \alpha^{\frac{1}{2} y(y-1)},$$

$$\overline{c} = \begin{pmatrix} a^x b^y \alpha^z \\ a^{x+y} b^y \alpha^{x+z+\frac{1}{2} y(y-1)} \end{pmatrix},$$

$$\overline{c} = [x+y, y, x+z+\tfrac{1}{2} y(y-1)],$$

$$\overline{c}^2 = [x+2y, y, x+y+x+z+\tfrac{1}{2} y(y-1)]$$

$$= [x, y, z+y(y-1)] = (x, y, z),$$

car $y(y-1)$ *est pair.*

$$\overline{ac} = [x+y, y, x+y+z+\tfrac{1}{2} y(y-1)],$$

$$\overline{bc} = [x+y, y, z+\tfrac{1}{2} y(y-1)],$$

$$\overline{abc} = [x+y, y, y+z+\tfrac{1}{2} y(y-1)].$$

Ensuite

$$\overline{d} = \left[\begin{matrix} a^x b^y \alpha^z \\ b^x (ab)^y \alpha^z \end{matrix}\right],$$

$$\begin{matrix} (ab)^y = a^y b^y a^{\frac{1}{2}y(y-1)}, \\ b^x a^y = a^y b^x \alpha^{xy}, \end{matrix} \qquad \overline{d} = \left(\begin{matrix} a^x b^y \alpha^z \\ a^y b^{x+y} \alpha^{z+xy+\frac{1}{2}y(y-1)} \end{matrix}\right),$$

$$\begin{aligned}
\overline{d} &= [y, x+y, z+xy+\tfrac{1}{2}y(y-1)], \\
\overline{ad} &= [y, x+y, y+z+xy+\tfrac{1}{2}y(y-1)], \\
\overline{bd} &= [y, x+y, x+z+xy+\tfrac{1}{2}y(y-1)], \\
\overline{abd} &= [y, x+y, x+y+z+xy+\tfrac{1}{2}y(y-1)], \\
\left\{\begin{matrix} \overline{cd} \\ \overline{cd} \end{matrix}\right. &\begin{matrix} = [y, x+2y, x+z+\tfrac{1}{2}y(y-1)+xy+y^2+\tfrac{1}{2}y(y-1)], \\ = [y, x, x+z+xy) \qquad [\text{car } y(y+1) \text{ est pair}], \end{matrix} \\
\left\{\begin{matrix} \overline{acd} \\ \overline{acd} \end{matrix}\right. &\begin{matrix} = [y, x+2y, x+y+z \\ \quad +\tfrac{1}{2}y(y-1)+xy+y^2+\tfrac{1}{2}y(y-1)], \\ = [y, x, x+y+z+xy), \end{matrix} \\
\left\{\begin{matrix} \overline{bcd} \\ \overline{bcd} \end{matrix}\right. &\begin{matrix} = [y, x+2y, z+\tfrac{1}{2}y(y-1)+xy+y^2+\tfrac{1}{2}y(y-1)], \\ = (y, x, z+xy), \end{matrix} \\
\left\{\begin{matrix} \overline{abcd} \\ \overline{abcd} \end{matrix}\right. &\begin{matrix} = [y, x+2y, y+z+\tfrac{1}{2}y(y-1)+xy+y^2+\tfrac{1}{2}y(y-1)], \\ = (y, x, y+z+xy), \end{matrix} \\
\left\{\begin{matrix} \overline{d}^2 \\ \overline{d}^2 \\ \overline{d}^2 \end{matrix}\right. &\begin{matrix} = [x+y, x+2y, z+xy \\ \quad +\tfrac{1}{2}y(y-1)+xy+y^2+\tfrac{1}{2}(x+y)(x+y-1)], \\ = [x+y, x, z+\tfrac{1}{2}y(y-1)+\tfrac{1}{2}(x+y)(x+y-1)], \\ = \{x+y, x, z+\tfrac{1}{2}[x^2+2xy-x+2y(y-1)]\}, \end{matrix} \\
\overline{d}^2 &= [x+y, x, z+\tfrac{1}{2}x(x-1)], \\
\overline{ad}^2 &= [x+y, x, y+z+\tfrac{1}{2}x(x-1)], \\
\overline{bd}^2 &= [x+y, x, x+z+\tfrac{1}{2}x(x-1)], \\
\overline{abd}^2 &= [x+y, x+y+z+\tfrac{1}{2}x(x-1)], \\
\left\{\begin{matrix} \overline{cd}^2 \\ \\ \overline{cd}^2 \end{matrix}\right. &\begin{matrix} = [x+2y, x+y, x+z+\tfrac{1}{2}y(y-1)+\tfrac{1}{2}(x+y)(x+y-1)] \\ = \{x, x+y, x+y+z+\tfrac{1}{2}[2y(y-1)+x^2+2xy-x)\}, \\ = [x, x+y, x+y+z+\tfrac{1}{2}x(x-1)], \end{matrix}
\end{aligned}$$

$$\left\{\begin{aligned}\overline{acd}^2 &= [x+2y, x+y, x+y+z \\ &\qquad + \tfrac{1}{2}y(y-1) + \tfrac{1}{2}(x+y)(x+y-1)] \\ &= [x, x+y, x+z+\tfrac{1}{2}x(x-1)],\end{aligned}\right.$$

$$\left\{\begin{aligned}\overline{bcd}^2 &= [x+2y, x+y, z+\tfrac{1}{2}y(y-1)+\tfrac{1}{2}(x+y)(x+y-1)] \\ &= [x, x+y, y+z+\tfrac{1}{2}x(x-1)],\end{aligned}\right.$$

$$\left\{\begin{aligned}\overline{abcd}^2 &= [x+2y, x+y, y+z+\tfrac{1}{2}y(y-1)+\tfrac{1}{2}(x+y)(x+y-1)] \\ &= [x, x+y, z+\tfrac{1}{2}x(x-1)].\end{aligned}\right.$$

Résumé :

$$1, \quad (x, y, y+z), \quad (x, y, x+z), \quad (x, y, x+y+z);$$
$$[x+y, y, x+z+\tfrac{1}{2}y(y-1)], \quad [x+y, y, x+y+z+\tfrac{1}{2}y(y-1)],$$
$$[x+y, y, z+\tfrac{1}{2}y(y-1)], \quad [(x+y, y, y+z+\tfrac{1}{2}y(y-1)],$$
$$[y, x+y, z+xy+\tfrac{1}{2}y(y-1)], \quad [y, x+y, y+z+xy+\tfrac{1}{2}y(y-1)],$$
$$[y, x+y, x+z+xy+\tfrac{1}{2}y(y-1)],$$
$$[y, x+y, x+y+z+xy+\tfrac{1}{2}y(y-1)],$$
$$(y, x, x+z+xy), \quad (y, x, x+y+z+xy),$$
$$(y, x, z+xy), \quad (y, x, y+z+xy),$$
$$[x+y, x, z+\tfrac{1}{2}x(x-1)], \quad [x+y, x, y+z+\tfrac{1}{2}x(x-1)],$$
$$[x+y, x, x+z+\tfrac{1}{2}x(x-1)], \quad [x+y, x, x+y+z+\tfrac{1}{2}x(x-1)],$$
$$[x, x+y, x+y+z+\tfrac{1}{2}x(x-1)], \quad [x, x+y, x+z+\tfrac{1}{2}x(x-1)],$$
$$[x, x+y, y+z+\tfrac{1}{2}x(x-1)], \quad (x, x+y, z+\tfrac{1}{2}x(x-1)].$$

C'est un groupe isomorphe au groupe symétrique de quatre lettres.

TABLE.

Pages.

Quelques démonstrations relatives à la théorie des nombres entiers complexes cubiques..... 1

Propriétés de quelques groupes d'ordre fini..... 23

PARIS. — IMPRIMERIE GAUTHIER-VILLARS,
40176 Quai des Grands-Augustins, 55.

UNIVERSITY OF ILLINOIS-URBANA
512.74L57Q C001
QUELQUES DEMONSTRATIONS RELATIVES A LA T
3 0112 017077881